S. HRG. 103–1067

THE ADMINISTRATION'S CLIPPER CHIP KEY ESCROW ENCRYPTION PROGRAM

THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

ON

THE ADMINISTRATION'S IMPLEMENTATION OF A PROGRAM TO ENABLE THE GOVERNMENT TO DECODE FORMS OF COMMUNICATION THAT IS ENCRYPTED WITH A COMPUTER CHIP CALLED "CLIPPER CHIP"

MAY 3, 1994

Serial No. J–103–55

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
20–486 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-047780-8

S. HRG. 103–1067

THE ADMINISTRATION'S CLIPPER CHIP KEY ESCROW ENCRYPTION PROGRAM

THE

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED THIRD CONGRESS

SECOND SESSION

ON

THE ADMINISTRATION'S IMPLEMENTATION OF A PROGRAM TO ENABLE THE GOVERNMENT TO DECODE FORMS OF COMMUNICATION THAT IS ENCRYPTED WITH A COMPUTER CHIP CALLED "CLIPPER CHIP"

MAY 3, 1994

Serial No. J–103–55

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
20–486 CC WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0–16–047780–8

COMMITTEE ON THE JUDICIARY

JOSEPH R. BIDEN, JR., Delaware, *Chairman*

EDWARD M. KENNEDY, Massachusetts
HOWARD M. METZENBAUM, Ohio
DENNIS DECONCINI, Arizona
PATRICK J. LEAHY, Vermont
HOWELL HEFLIN, Alabama
PAUL SIMON, Illinois
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
CAROL MOSELEY-BRAUN, Illinois

ORRIN G. HATCH, Utah
STROM THURMOND, South Carolina
ALAN K. SIMPSON, Wyoming
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
HANK BROWN, Colorado
WILLIAM S. COHEN, Maine
LARRY PRESSLER, South Dakota

CYNTHIA C. HOGAN, *Chief Counsel*
CATHERINE M. RUSSELL, *Staff Director*
MARK R. DISLER, *Minority Staff Director*
SHARON PROST, *Minority Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY AND THE LAW

PATRICK J. LEAHY, Vermont, *Chairman*

HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California

ARLEN SPECTER, Pennsylvania
LARRY PRESSLER, South Dakota

BRUCE COHEN, *Chief Counsel/Staff Director*
RICHARD HERTLING, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIAL SUBMITTED

APPENDIX

Additional Submissions for the Record

Page

QUESTIONS AND ANSWERS

THE ADMINISTRATION'S CLIPPER CHIP KEY ESCROW ENCRYPTION PROGRAM

TUESDAY, MAY 3, 1994

U.S. SENATE,
SUBCOMMITTEE ON TECHNOLOGY AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:39 a.m. in room G50, Dirksen Senate Office Building, Hon. Patrick J. Leahy (chairman of the subcommittee), presiding.

Present: Senators Specter, Pressler, and Murray [ex officio].

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Good morning. We are holding today's hearing for a number of reasons. The administration is implementing a controversial program to enable the government to decode any telephone, fax, or computer communication that is encrypted with a special computer chip called Clipper Chip. In doing so, and I understand the reasons for this, the administration has responded to the alarm bells that were sounded by our law enforcement and intelligence agencies. They are struggling to keep pace with emerging telecommunications technologies that make it easier to encrypt messages and evade lawful wiretaps.

Incidentally, the administration, has stressed, and I am sure will in testimony today, the security of Clipper Chip. The price for this security is that two Federal agencies will hold a duplicate set of keys to decode any communication encrypted with the Clipper Chip before any wiretap order has been issued.

Now, before American citizens and potential customers of American computer and telecommunications products will see this as the solution to privacy or security concerns, they have got to be assured that iron-clad procedures are in place. We have got to be able to guarantee that, absent a court order, no one is going to be able to decode their private communications except, of course, the person they want to. Otherwise, even law-abiding users are not going to want to use encryption devices with Clipper Chip.

We are going to see demonstrations of how encryption works and we are going to hear from government witnesses, experts and critics of Clipper Chip. I would note, that a recent Time/CNN poll indicated that 80 percent of the American people oppose this program, so I would hope that the public might get a chance to hear more about it today.

Admiral McConnell, I want to thank you for your willingness to be here. I understand that, as we have discussed before, you have to limit your public remarks out of concern for national security. A second part of this hearing will be held in a secure room so that we can hear the remainder of your remarks.

Now, our Constitution requires that we strike a balance between an individual's right to be left alone and conduct his or her own affairs without government interference, and our interest in a secure and safe society. The Clinton administration's Clipper Chip may be seen as a solution by the law enforcement and intelligence agencies, but it raises a whole lot of questions for its potential users about whether it tips that fundamental balance.

I have got to tell you I have some real questions about whether any sophisticated criminal or terrorist organization is going to use the one code endorsed by the U.S. Government and for which U.S. Government agents hold the decoding keys, especially when there are a number of alternative encryption methods commercially available, including one I read was just recently sent out over the Internet.

I am concerned about the Clipper Chip's impact on the competitiveness of our robust high-tech industries. We have got to ensure that it does not impede American companies trying to market high-tech products overseas. The administration's steps to reform some export restrictions on encryption and telecommunications technology is welcome, but we have to talk about that.

I would note that we are talking today about Clipper Chip and not about digital telephony. Many get the two mixed up, and, in a way, some of the political questions are the same. In digital telephony, the question is whether we will be able to hold up advances in communications technology until the Justice Department can be assured that they have a way of conducting lawful wiretaps on that.

The administration is asking the same thing with Clipper Chip: That we not be allowed to develop and export encryption devices until the government is given the keys to be able to decode encrypted messages under appropriate standards and court orders.

My concern, I have got to tell you frankly, is what happens if we say that the Federal Government is empowered to sign off on technology and technology may not go forward until they do. It bothers me very much because my experience with the Federal Government has been that in the areas of computers and telecommunications the Federal Government has carefully and assiduously stayed at least 10 to 20 years behind the curve on just about everything.

You can make a better and clearer telephone call from the Washington-to-New York shuttle than you can from Air Force 1, with all its expensive equipment. Most telephone systems of the Federal Government, as installed, have been antiquated. The only distinction is they usually pay far more than they would if they just bought it off the shelf. You see the FAA struggling with a computer system where they have to buy tubes from eastern European countries because nobody with advanced technology even makes the darn things anymore.

If this is the same government that will sign off on when we go forward, I can see the United States being in the backwash of computer and telecommunications technology. I don't want to see that happen. I suspect that none of the witnesses from the government want to see that happen either.

So we have two problems, really. We have the problem of those who are concerned about what Clipper Chip might do to our technological competitiveness in this country and, of course, we have the further problem, as pointed out by the 80 percent of the people who responded that way in the Time/CNN poll, of privacy.

The information superhighway holds the promise of an information explosion that is going to enhance our marketplace of ideas, bringing untold benefits to our citizens. But this promise will be an empty one unless people are sure that when they go online or talk on the phone they are not forfeiting important fundamental rights, like their right to privacy.

New technologies present enormous opportunities for Americans, but we have got to strive to safeguard our privacy if these technologies are to prosper in this information age. Otherwise, in the service of law enforcement and intelligence needs, we are going to dampen any enthusiasm Americans may have for taking advantage of the new technology.

I come from a law enforcement background. I spent 8 years on the Senate Intelligence Committee and continue to be involved with intelligence agencies through my Appropriations Committee hat. I understand the tremendous problems, especially with organized crime, that law enforcement faces, and the tremendous problems, especially with terrorism and the potential threat of terrorism, that our intelligence agencies face. But I also know that this country has to survive economically, and one of the ways we do so is the fact that we have been able to have certain technological advances. I don't want that to change.

We will go first, Ms. Harris, to you, and then to Mr. Kammer, who is going to do a demonstration. Ms. Harris is Assistant Attorney General of the Criminal Division at the Department of Justice, and I am delighted you are here.

PANEL CONSISTING OF JO ANN HARRIS, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE; AND RAYMOND G. KAMMER, DEPUTY DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

STATEMENT OF JO ANN HARRIS

Ms. HARRIS. Thank you, Mr. Chairman, and thank you for the opportunity to talk with you about the key escrow encryption concept. In particular, I want to talk about balancing the public's right to the best protection that technology can provide for legitimate communications—balancing that with the public's right to be protected from criminals and terrorists, and I want to talk about how we can maintain the balance in this age when technology is, as you have noted, exploding all around us.

As I know you understand, many groups engaged in the most serious and violent criminal conduct, including drug traffickers and organized crime groups, major street gangs and terrorist groups,

must have a means of communicating quickly, over distance, with each other. They rely on telephonic communications to conduct their illicit activities, and at this time the law permits law enforcement to obtain court orders to tap into these criminal conversations upon, of course, a stringent showing of necessity and a showing of probable cause that the communications are criminal in nature.

Even though we use that power very sparingly, our ability to hear and, importantly, to understand these conversations has been crucial to effective law enforcement. Evidence from electronic surveillance has resulted in the convictions of, we estimate, 22,000 felons in the last decade.

As a Federal trial lawyer specializing in criminal cases, I can tell you from plenty of first-hand experience and knowledge that some of the most powerful evidence I have ever seen or heard in court against these criminals are recordings of their own words directing their criminal enterprises in a way that a jury can understand.

Further, I know from experience recently that authorized wiretaps have not only caught and convicted criminals, they have saved lives, including kidnaping victims and targets of terrorist activities. For example, in four separate instances in the very recent past, law enforcement has obtained critical information about the identity of kidnapers who were threatening immediate harm to hostages. Law enforcement has learned the location of the hostages and was able to move-in and rescue the hostages before harm was done. These are fast-moving scenarios where our ability to get up on a wiretap and understand the content of the conversations in realtime is absolutely critical.

With court-authorized interception of telephone conversations, we have penetrated the highest levels of mob activity, narcotics trafficking. We have brought down whole organizations. Cases come to mind that everyone, I think, has heard of. The *Pizza Connection* case, the *Commission* case, the *Hererra-Botrega* case involving the Cali cartel, are just examples of the power of the wiretap as a law enforcement tool, and it is not limited to just mobs and drugs. *Operation Ill Wind,* for example, was a Defense procurement fraud case in which wiretaps led to 45 search warrants, 60 convictions, hundreds of millions of dollars recovered in fines.

In addition, wiretaps have helped us prosecute child pornography cases, murder-for-hire schemes. They have permitted us to make seizures of tons of illicit drugs, helped us follow and seize the illicit millions of dollars made by traffickers, without compromising ongoing investigations.

But, Mr. Chairman, the ability to intercept these communications is only the first step. We must have the ability to understand the content of these lawfully authorized wiretaps in order to act. If we intercept illicit communications in a foreign language, we need to bring in a translator who knows the language. If the language is guarded, as it frequently is in these intercepted criminal conversations, we need to bring in an expert to tell us what it means.

Critical to my point here is if intercepted criminal conversations are encrypted, we need the ability to cut through the encryption, just as we need a translator to cut through the foreign language. If we can't cut through the encryption in the coming age of tech-

nology, law enforcement efforts will be seriously hampered. This ability to understand the words that we are lawfully intercepting pursuant to court order is all we seek with the Clipper Chip, no less and no more.

Mr. Chairman, the plain fact is, as you have noted, that high-quality voice encryption in an affordable, portable, easy to use form will soon be widely available on the market. We anticipate that many legitimate users will acquire these and similar devices with the perfectly legitimate goal of protecting their personal and business confidential information. We worry, however, that such devices will also be used by criminal organizations to shield their illegal enterprises.

Mr. Chairman, last year, as you know, the Clinton administration, looking ahead to the future, trying to stay ahead of the curve, sought to address both of these important issues—the protection of legitimate communications without losing our ability to intercept criminal communications with key escrow encryption.

Key escrow encryption has two fundamental features. First, on the encryption side, to protect communications it uses a very strong algorithm, so strong that it can only be decrypted with a key that is unique to each individual key escrow encryption chip. Second, on the decryption side, to ensure the public of the privacy afforded by the key escrow encryption, this unique key is split into two components, each held by one of two independent entities serving as escrow agents. Those two entities are not permitted to release key components except to government agencies and, importantly, only to government agencies when they are already authorized by law to intercept the communications.

Mr. Chairman, we have worked to develop procedures that strike the right balance between the rigorous protection of the privacy of communications and the need in critical moments to be able to decrypt such communications in order to protect lives and preserve the public safety.

Clipper Chip key escrow encryption provides a combination of procedural requirements, technical safeguards and audit capabilities which will assure the integrity of the Key Escrow Encryption System without frustrating the ability of government agencies to understand encrypted communications in the course of lawful wiretaps.

Senator LEAHY. What happens if it is misused? Is there any recourse by somebody whose communication was intercepted? Suppose it was misused. We always assume law enforcement does these things according to court order, but we know that there has been misuse of taps before. What if that happened under this? Is there any way we can go back against the person? I understand the Attorney General has suggested that the escrow agents be immune from liability for mishandling the keys. Is that a good idea?

Ms. HARRIS. If I may, Mr. Chairman, first address the unlikelihood of that ever happening, given the protections built into the system——

Senator LEAHY. Let us assume the unlikelihood for the purposes of my question. Assume the unlikelihood that it were to happen; unlikely things sometimes do. After 20 years in this branch of the Federal Government, I have seen an awful lot of unlikely things

happen. I have seen Presidents declare that no money was diverted to the contras. I have seen statements before the Persian Gulf War that were false, and the American people spent $1.9 billion on foreign aid to Saddam Hussein as a result of misstatements to the American public.

I mean, things do happen, so let us just assume that one time out of a gazillion something went wrong. Is the Attorney General right in saying that the escrow agents should be immune from liability for mishandling the keys?

Ms. HARRIS. Mr. Chairman, I am not sure that the Attorney General has made such a statement with respect to immunity.

Senator LEAHY. What she said was the procedures do not create and are not intended to create any substantive rights for individuals intercepted through electronic surveillance.

Ms. HARRIS. All right. They are not intended to create any substantive rights for people intercepted any more than the present wiretap laws are intended to create substantive rights for people who are unlawfully intercepted. We are building in such protections that I find it unlikely this will happen, but let me say this, Mr. Chairman. It is a violation of Federal law right now illicitly to wiretap. We take that law very seriously. We will enforce that law.

Senator LEAHY. Would it be a violation of the same Federal law illicitly to use the Clipper chip keys?

Ms. HARRIS. I would have to look at it more carefully.

Senator LEAHY. Should it be?

Ms. HARRIS. Sorry?

Senator LEAHY. Would you see any problem in applying the same law to the misuse of Clipper chip keys as we apply to the misuse of wiretap today?

Ms. HARRIS. If, in fact, in the course of an illicit electronic surveillance, somehow a person got ahold of both aspects of the Clipper Chip, had the decryption device so that things were fed into it and somehow they were able to break into this system, it is unlawful to participate in illicit electronic surveillance. It depends on the facts of the case beyond that, Mr. Chairman, but I believe that if that occurs it is going to violate the law.

Senator LEAHY. Ms. Harris, a concern about Clipper Chip is that the government has the keys to that. But there are other encryption systems that are pretty good now, are there not, that you as the head of the Criminal Division are faced with?

Ms. HARRIS. My understanding is that the Clipper Chip is so much more powerful than anything available at this time that the Clipper Chip is a spectacular way of encrypting conversations. There are certainly other devices on the market now.

Senator LEAHY. What about Pretty Good Privacy, PGP? There was an article about that in the Wall Street Journal last week. And the Wall Street Journal, at least on their news items, are usually pretty accurate. Their editorials are written on a different planet. [Laughter.]

But in their article, they suggest if I recollect it correctly, that PGP is just about impossible to break. Is that right?

Ms. HARRIS. Well, the interesting thing about that particular device, as I understand it, is that it is software in a computer and does not reach phone bands; that is, voice bands, which is what

Clipper Chip is all about. I mean, what Clipper Chip is involved with is the encryption and decryption of the voice band.

Senator LEAHY. But that would be fairly easy to do. I mean, if much of our voice communications are now being digitized anyway, wouldn't it be fairly easy to run this through a computer program if somebody wanted to? If you can build it for data transmission in Pretty Good Privacy, wouldn't it be fairly easy to do it, or assume that that is going to be done within a relatively short time for voice transmission?

Ms. HARRIS. My understanding is that it is ever so much more complicated to do this with voice band, but I defer to the experts who are with me on the technology here.

Senator LEAHY. Well, let me ask you this question. I read an article about a convicted pedophile in California who used Pretty Good Privacy to encrypt his computer diary, which frustrated the police, who thought the computer diary might contain clues about a child pornography ring, something that I think all of us would agree that if law enforcement could find out about such a thing, we would want them to be able to take action.

Have you seen many such instances of encrypted communications?

Ms. HARRIS. Well, let me again address the child pornography case in California, which I think is the Wall Street Journal article, and just underline that that is computer software and that is not what we are talking about here. What I am talking about is our ability to understand intercepted voice communications at a time when we already have the court orders to intercept it, and——

Senator LEAHY. Well, let us——

Ms. HARRIS. I am sorry, Mr. Chairman.

Senator LEAHY. No, no; go ahead.

Ms. HARRIS. I was going to then answer your question. The fact is that at this particular point in time law enforcement has not been frustrated by, or significantly frustrated by voice band encryption. My point is, and you certainly underlined it in your remarks, Mr. Chairman, that we are trying to anticipate and get ahead of the curve on this particular subject because we understand the significance to law enforcement if, in fact, encryption devices as powerful as Clipper Chip are out there without our ability, under very circumscribed circumstances, to intercept and understand criminal conversations.

Senator LEAHY. We are going to demonstrate for you here a laptop computer with a computer software that encrypts voice communications. I appreciate what you said about the administration wanting to be ahead of the curve and I think in a lot of these communications and computer matters this administration has worked to get ahead of the curve. But don't think that Clipper Chip is just going to be used in normal straight voice communications because people can put these encryption devices through their computers and run it that way.

What I would ask is, about 900 wiretaps are conducted annually?

Ms. HARRIS. I think the figure in 1992, which is the last time we have figures, is 919.

Senator LEAHY. Did many of them involve encrypted conversations?

Ms. HARRIS. The short answer is no. Our concern is clear, Mr. Chairman, that if these devices explode on the market, as we believe they will, we will begin to be truly frustrated and unable to read criminal conversations.

Senator LEAHY. We are talking about the Clipper Chip. Why would a criminal organization or a terrorist organization buy something that has Clipper Chip in it for their encryption when they can buy other non-government-authorized systems that are also going to be extraordinarily difficult to crack, and perhaps impossible?

Ms. HARRIS. There are two answers to that, Mr. Chairman, and the first is—and this is just so true. I mean, why do they use telephones now? I mean, we are able to intercept and obtain invaluable evidence with court-authorized wiretaps because those kinds of organizations, knowing that we tap, continue to use the telephones.

I think the second answer to your question is that this is not easy, but our sense is that the Clipper Chip technology is so far advanced than anything else on the market or anything coming down the road that it will be regarded both by legitimate people and by illicit criminals as so powerful an encryption device that they will purchase it, that it will be something that they will want to use.

Senator LEAHY. But if I was sitting up at my farm in Vermont and running an international heroin, gun smuggling, and counterfeit Ben and Jerry's organization, why wouldn't I just buy Pretty Good Privacy, PGP, and just do it all by computer and fax? I mean that seriously. Why wouldn't I just do that and say the heck with you, and I could run it on the Internet?

Ms. HARRIS. Because right now, and I think for the foreseeable future, the Clipper Chip is such a more powerful encryption device that I would want, if I were you, to buy the best, and you, being quite confident that the Feds would never catch up with you, would want the best as well.

Senator LEAHY. But that is my point. Suppose I really am confident they are not going to catch me and I am really doing something very serious. Say I am in a rural location in the United States and I am running an international drug ring, something where there is enormous amounts of money so I can do whatever I want and buy whatever I want. Why would I buy something with Clipper Chip in it that comes, in effect, with a sign on it saying the Federal Government holds the keys to decipher this?

Ms. HARRIS. Let me again respond in two ways. First of all, you also will want to be making encrypted communications with legitimate organizations, with banks, with other legitimate organizations, to send your messages, to move your illicit money out of the country, to do a number of things. If the Clipper Chip technology is purchased by legitimate people in this country because it is the best technology, then you—shall we change our analogy—then the criminal who is sitting up on a farm in Vermont is going to need to communicate with those devices that the legitimate——

Senator LEAHY. If he wants to move money from the Chase Manhattan Bank to the Zurich National Bank, what you are saying is there he would have to—because they were using Clipper Chip, he would have to use Clipper Chip?

Ms. HARRIS. Let us go to *Ill Wind.* I mean, to the extent that we have a defense procurement fraud case and we have people trying to communicate with defense organizations and with legitimate companies, if you believe—that is, if the drug trafficker up in Vermont believes that the only way that he can interact with other independent entities with encryption devices is to also buy Clipper Chip, he is going to do it.

I suppose the second part of the answer is that to the extent that this powerful encryption algorithm is one which manufacturers decide to market because it is the very best, then I suppose that the market for lesser devices is not going to be that great. It is not going to be cost effective to produce those kinds of encryption devices.

Senator LEAHY. Of course, this also assumes that these legitimate commercial organizations outside the United States are going to want to use some kind of a standard for encryption that they know the United States hold the keys, as compared to trying to find some other standard created by some other country for which the United States would not hold the key. We would see people in this country buying the other country's technology. That is at least a possibility?

Ms. HARRIS. Anything is possible. These are not easy issues, and I will absolutely say that. There is something, though, that I think needs be said perhaps not exactly in that context, but I think I need to underline time and again, from our perspective what we are talking about is already court-authorized interceptions of communications, and that all Clipper Chip does—after a court has already authorized the interception of the communication, all that is happening here is that we are getting the ability to understand the content of those legitimately intercepted communications.

Senator LEAHY. Well, as I understand it, the escrow agents release the keys when they get two faxes, one from the prosecutor saying a wiretap order exists, and one from the law enforcement agency requesting the keys for a particular chip I.D. number for which they say they have a wiretap order. Now, the escrow agents themselves never see this court order, is that correct?

Ms. HARRIS. It is correct that the escrow agents never see it themselves, and let me explain why. Certainly, they have to certify that there is a court order. Incidentally, the request—let us put it this way: If DEA has a court-authorized wiretap up intercepting the kinds of communications that I have already talked about that are important and very criminal in nature, and if they hit some white noise that sounds as if it is encrypted, law enforcement has a decrypt device through which it can run a tape or the realtime noise through and that little box will tell DEA that this is a Clipper chip-encrypted conversation, and it will give DEA an encoded number coming off the chip.

That DEA agent and his supervisors will then communicate to each of the independent escrow agents and certify that there is a court order already in place authorizing them to intercept this communication; that it is a key escrow-encrypted conversation; that here is the number of the chip. This is going to the independent escrow agents, and the court order will terminate—that is, our ability to intercept will terminate at such-and-such a date. Please com-

municate back to our decrypt device the two pieces of the key that will enable our decrypt device to decode the conversation so that we may get it in realtime.

Senator LEAHY. You could get it in realtime, then?

Ms. HARRIS. We need it in realtime.

Senator LEAHY. Then how do those keys then get returned to the escrow agent?

Ms. HARRIS. My understanding is that right now with the prototype, we will have to manually destruct the keys that are in the encrypted box at the time that our authorization to intercept the communications ends pursuant to court order. As this develops, Mr. Chairman, and we are working through it right now, as I understand it, there will be a way that they will self-destruct at the particular time at the end of the court-ordered interceptions.

Senator LEAHY. So nothing gets returned to the escrow agents?

Ms. HARRIS. That is correct. Now, I should say that there are, as you know, in our procedures substantial auditing requirements, substantial recordkeeping requirements. I should have said as well that after the DEA agent makes his faxed request to both of the independent escrow agents and the process starts back in realtime, it is required that the Federal prosecutor in charge of this case contact the key escrow agents and confirm all of the certification that has been put forth by the agent.

Senator LEAHY. Now, this decryption device, the one that at least puts the first trigger up to say your white noise is a Clipper Chip, and number whatever——

Ms. HARRIS. That is right.

Senator LEAHY. Have those devices been made yet?

Ms. HARRIS. There is one.

Senator LEAHY. I mean, how many of these are we going to have? Are you going to have to have them all over the country?

Ms. HARRIS. Well, I think that we must—and we are very respectful of this—we must keep very, very careful control of the number of encryption devices. They are the kinds of items that I don't think anyone would want spread all over the country.

Senator LEAHY. Well, say, you have got a case in Tucson, AZ, and you have got one in Burlington, VT, and Abilene, KS. I mean, these are geographically kind of spread around. In each one of these areas, one might assume that law enforcement, at least for the rudimentary type of wiretaps, have equipment to do that, but one decrypt device might not do them any good.

Ms. HARRIS. I mean, we are working through these issues right now and are very, very sensitive to the fact that we do not want proliferation of these decrypt devices. I believe that the technology is such, or at least we are working on it, where you could transmit the white noise to the box in a centrally located place and get the answer.

Senator LEAHY. How big is this decryption device going to be? I assume it is something relatively small.

Ms. HARRIS. It is not huge. When I said small box to my staff, they said, well, it is not small.

Senator LEAHY. Bigger than a bread box, smaller than a——

Ms. HARRIS. I think it is about the size of—I was just getting ready to say, and my able staff says, it is a PC. It is that size.

Senator LEAHY. Do you and the administration see any need for new legislation to implement your Clipper Chip proposal?

Ms. HARRIS. The short answer is no.

Senator LEAHY. So you are ready to just go ahead, no matter what we might think here?

Ms. HARRIS. Well, we always very, very carefully consider what is said here.

Senator LEAHY. Yes, yes, yes. [Laughter.]

Ms. HARRIS. But let me go further, Mr. Chairman. Again, if you look at it the way that I have described, what we are talking about is simply a more sophisticated way to understand more sophisticated coding of criminal conversations.

Senator LEAHY. Wearing my hat from another committee, there is one part, though, you may have some interest in talking to us about. How much is this thing going to cost?

Ms. HARRIS. I think you know that to the extent that the Department has already invested in these devices for law enforcement——

Senator LEAHY. No, but just running the escrow system is going to cost you millions of dollars a year, won't it?

Ms. HARRIS. I don't have easy estimates on that, Mr. Chairman.

Senator LEAHY. Wearing the other hat from the Appropriations Committee, we may be looking at some legislation. Do you think that as part of the reporting requirements, the Justice Department should give Congress a full accounting of where these decrypt devices are? I mean, these things are set up so they can unlock a coded serial number. They can get direct transmission of the keys from the escrow agents. They can use the keys to decrypt clipper-encrypted conversations. Do you think there should be any reporting requirement of where they are?

Ms. HARRIS. Well, I mean certainly there should be a reporting requirement, and what we intend to do is two things, really. We intend to report to the Administrative Office of U.S. Courts where we already report all of our court-authorized wiretaps. We will certainly report there that a wiretap was encrypted and decrypted with key escrow encryption.

Also, my understanding is that to the extent that the intelligence committees are giving oversight that the information would be made available to them. We assume the Administrative Office of U.S. Courts is going to report to Congress, as it does every year.

Senator LEAHY. If you say there is no legislation required, I would assume that the Justice Department at least anticipates regulations being promulgated?

Ms. HARRIS. What we have done, and I will be happy to go through it in more detail, is we have promulgated internal regulations that are designed to assure that the integrity of this system will be protected. What it does is internally guide us in terms of the process by which our agents go to get the keys, certify the process by which the keys come back, the process by which we audit very carefully. We plan to audit every single encryption instance.

Senator LEAHY. Would the AG be able to change the set of escrow agents after the initial selection?

Ms. HARRIS. It is not——

Senator LEAHY. Suppose you have got an escrow agent who says, wait a minute, I think this is wrong, I don't think that this key

should be released. Could the Attorney General just say, well, then we are going to get a different escrow agent?

Ms. HARRIS. Well, let me say a couple of things. One, we are still open and looking at the options with respect to escrow agents. But, two, it is really very important that there be some continuity once the escrow agents are in place. It is not contemplated that, with the appropriate certification, the escrow agent, other than looking at the certification and saying this is not enough, this is wrong—I don't think that you will find the Attorney General wanting to change escrow agents simply because one said no.

Senator LEAHY. Well, stranger things have happened. I worry about the security of the system. If I understand this correctly, every Clipper Chip has the same family key programmed into it. Law enforcement uses the family key to decode the intercepted serial number which the targeted chip sends out, I guess, at the beginning of every conversation. If they have that, they can get the government's duplicate set of decoding keys from the escrow agents following the normal procedure.

If they have got the decrypt device, the initial step, at least, can be done by anybody who has got one of the devices. I mean, let us assume that it has happened on occasion that illegal wiretaps have been done even by law enforcement. If they have got the initial decrypt device, they can at least have the family key or the number.

Now, they can't get the decoding keys unless the escrow agents give them to them. Of course, without drawing this out too far, somebody had to make the decoding keys for the escrow agents. Somewhere, they are out there—that is what I am getting to, or the potential is out there.

Ms. HARRIS. But the potential is so minuscule. I mean, the protections that are built into this system to give everyone the assurance that no single person can illicitly get into this system. I must say with respect to the family codes, even if you got that, because those are coded, you wouldn't be able to get the number to send off to the escrow agents, as I understand it.

I mean, we are talking about independent escrow agents. We are talking about a requirement that a prosecutor go back to the escrow agents and confirm all the certifications. I mean, we built it in both mechanically and humanly that there are checks and doublechecks and doublechecks.

Senator LEAHY. If you have the decrypt device, even if you don't know what I am saying, you at least know who I am because you know the unique I.D. number of the device I am calling from.

Ms. HARRIS. I don't think I would know where you were calling from, even. I would know a number, period. I would not be able to track the number.

Senator LEAHY. We have several ongoing reviews; let me make sure I have got them right. We have got a White House interagency working group, the NIST, and the National Research Council of the National Academy of Sciences. You haven't fully implemented the key escrow system or the decrypt device, to see how this works. Are we moving ahead of ourselves in this? Having expressed the earlier concern about the Federal Government always trying to stay care-

fully and traditionally behind the curve, are we getting a little bit ahead of the curve on this one?

Ms. HARRIS. Let me put it this way. The studies that you have alluded to, Mr. Chairman—the White House policy study is completed, and although one continues to study these matters and will continue to study them for as long as they are important, that is completed. The NIST part of this, as I understand it, although it is probably better addressed to Mr. Kammer, is completed. I don't know about the last study that you have alluded to, but I think we are moving at the appropriate speed. And, yes, speaking of the technology, we are attempting to stay ahead of the curve.

Senator LEAHY. If we allow American companies to export Clipper Chip to non-U.S. users, say a non–U.S. user in France, what happens when the French law enforcement or intelligence community calls up and says, "by the way, we are kind of worried about Harris Ltd. that has just set up in the Bordeaux region. We don't think they are just selling wine. Can we have the keys to tap in?"

Ms. HARRIS. I think that we must very, very carefully control this technology and the ability to use it. As I say, we have tried to put in place procedures that will assure that. I think, with respect to foreign law enforcement requests, a couple of things. One, I think we have to take it on a case-by-case basis, and I think that even on a case-by-case basis I think we have to consider very carefully keeping the technology and the hardware, for that matter, with us and just go ahead and do the translation for them; that is, give them the words, the decrypted words, but there is no reason for us to go beyond that.

[The prepared statement of Jo Ann Harris follows:]

PREPARED STATEMENT OF JO ANN HARRIS

Mr. Chairman members of the Subcommittee, I am pleased to be able to appear before you today to talk about a matter vital both to the protection of privacy and to the preservation of public safety.

As this Subcommittee understands quite well, many groups engaged in the most serious and violent criminal conduct—including drug traffickers, organized crime groups, and major street gangs—rely on electronic communications to conduct their illicit activities. Without the continued ability to conduct lawfully authorized wiretaps, law enforcement at the Federal, State, and local level will be seriously hampered in its ability to protect society from the depredations of these criminals.

Even though it is used sparingly, electronic surveillance has been crucial to effective law enforcement. Evidence from electronic surveillance has resulted in the convictions of more than 22,000 felons over the past decade. Indeed, without wiretaps, some extremely significant criminal activity could not be detected or properly investigated—much less successfully prosecuted. Wiretaps are not a routine investigative technique and are only used when other techniques have proven, or are likely to be, unsuccessful—often because those other techniques pose too great a risk to police or cooperating individuals. Wiretaps permit law enforcement authorities to penetrate closely controlled but highly sophisticated enterprises that might otherwise engage in wholesale criminal activity with impunity. Society cannot afford to lose the protection wiretaps afford it.

At the same time, technology is making it increasingly possible for individuals and private enterprise to protect the confidentiality of personal and proprietary information through the use of encryption—the electronic "scrambling" of communications. The market now offers high-quality voice encryption in an affordable, portable, easy-to-use form. We anticipate that many legitimate users will acquire these and similar devices to protect their confidential information; we worry, however, that such devices will also be used by criminal organizations to shield their illegal enterprises.

As you know, Mr. Chairman, last year the Clinton Administration sought to address both these important issues by announcing the availability of key-escrow

encryption (sometimes referred to as the "Clipper Chip"). Key-escrow encryption has two fundamental features. First, it uses an extremely strong algorithm, one 16 million times stronger than the Data Encryption Standard—DES—and so strong that law enforcement can only decrypt it with a key that is unique to each individual key-escrow encryption chip. Second, to assure the public of the privacy afforded by key-escrow encryption, that unique key is split into two components that are held by two independent entities serving as escrow agents. Those two entities may release key components only to government agencies when needed for lawfully authorized interceptions.

As the Administration has made clear on a number of occasions, the key-escrow encryption initiative is a voluntary one; we have absolutely no intention of mandating private use of a particular kind of cryptography, nor of criminalizing the private use of certain kinds of cryptography. We are confident, however, of the quality and strength of key-escrow encryption as embodied in this chip, and we believe it will become increasingly attractive to the private sector as an excellent, easy-to-use method of protecting sensitive personal and business information.

The Clinton Administration has been farsighted in seeing the advent of high-quality, user-friendly encryption products and the implications of such products. It has also been prepared to act early, when markets are still developing and when both consumers and manufacturers are seeking strong, reliable cryptography for use in mass-market products.

We believe, therefore, Mr. Chairman, that, as one major equipment manufacturer has already done, others will respond to their customers' needs for extremely strong encryption by marketing key escrow-equipped products. And as that occurs, we look for a gravitation of the market to key-escrow encryption, based on both a need for interoperability and a recognition of its inherent quality. Even many of those who may desire encryption to mask illicit activities will choose key-escrow encryption because of its availability, its ease of use, and its interoperability with equipment used by legitimate enterprises.

Mr. Chairman, let me speak about the key-escrow system in a bit more detail, beginning with the selection of the two entities that are serving as key escrow agents. In selecting escrow agents, we looked for a number of important qualifications. Among other things, the candidates needed to:

- Be experienced in handling sensitive materials;
- Be familiar with communications and computer issues;
- Be able to respond quickly, and around the clock, when government agencies need to have encryption keys issued to them; and
- Be generally regarded by the public as both reliable and effective.

Especially to get the system up and running, we believed it made sense to look to agencies of the Executive branch. In light of that consideration and the criteria I have just mentioned, the Commerce Department's National Institute of Standards and Technology (NIST) and the Treasury Department's Automated Systems Division appeared to be the two best candidates; and they have been so designated.

NIST, as you are well aware, has long experience in matters relating to protection of sensitive, unclassified information and, indeed, has been pivotal in the development of the key-escrow encryption initiative. Treasury's Automated Systems Division—which is not part of any of the Treasury law enforcement agencies—is a 24-hour a day operation that is well experienced in handling matters of the utmost sensitivity.

As you know, on February 4, 1994, the Administration made a number of announcements regarding encryption policy generally, and key-escrow encryption specifically. Among those announcements were the designation of the escrow agents and the publication of the procedures under which the escrow agents would be permitted to release key components:

- To Federal law enforcement authorities for use in wiretaps under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Title III);
- To State or local law enforcement authorities for use in wiretaps under state statutes; and
- To Federal agencies for use in wiretaps under the Foreign Intelligence Surveillance Act (FISA).

Let me describe for you the kinds of circumstances under which escrowed key components will be made available to government agencies when needed in conjunction with lawfully authorized wiretaps.

Mr. Chairman, as this Subcommittee well understands, Federal laws clearly lay out the circumstances in which wiretaps may be conducted, consistent with the Constitution. Wiretaps not lawfully authorized are criminal offenses—offenses that we take very seriously. Moreover, as the Subcommittee is aware, Federal law enforcement agencies may conduct wiretaps only for the most serious kinds of offenses and do so only after an extremely careful internal review of the need for, and the propriety of, a wiretap. That review process requires not only careful screening within the particular investigative agency—at both the local and headquarters level—but a thorough evaluation by a supervising prosecutor, usually an Assistant U.S. Attorney in the district in which the wiretap will be conducted. At each of those levels, there is a close review of the proposal to ensure that there is probable cause for the wiretap, that the case justifies use of this important technique, and that alternative techniques are not satisfactory. Finally, no Federal Title III application may proceed without approval at a senior level within the Department of Justice. I would also note that no FISA application may proceed without the approval of the Attorney General.

And, Mr. Chairman, that leads to the most important point which is that, whether for criminal or foreign intelligence purposes, the statutes require court authorization for wiretaps, even in the extremely rare cases in which they have begun under an emergency authorization. In a criminal case, the Government must show probable cause to believe that the telephone targeted is being used in furtherance of a specific serious Federal criminal offense. In a FISA case, the Government must show probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power and that the facility or place, such as the telephone, is being used by a foreign power or agent of a foreign power.

When we talk about access to escrowed components, therefore, we are talking about the ability of government agencies—Federal, State, or local—to decrypt communications when they are already lawfully authorized to intercept those communications as part of a wiretap. We are not talking about any change in the protection of the privacy of telecommunications. Nor are we talking about any additional authorization from the courts. The applicable statutes already permit government agencies that are authorized to conduct wiretaps to acquire the content of the intercepted communications and, if necessary, to translate or decode the communications as part of that process.

Let us assume, then, that government agents—DEA, for the sake of argument—are conducting a court-ordered wiretap and encounter unintelligible communications they think may be key-escrow encryption. What do they do? First, they can run the communications—live or on tape—through a so-called decrypt processor. The decrypt processor—a specially programmed and equipped personal computer—can tell the agents whether key-escrow encryption is being used and, if so, the unique ID number of the particular chip. This last point is critical, of course, because each chip has its own truly unique key; without knowing the ID number of the chip, the law enforcement agency cannot determine which key components to request.

Armed, however, with that information, they can submit a key component request to the two escrow agents, NIST and Treasury. In that request, they'll be required, among other things, to:

(1) Identify themselves and the agency they're with;

(2) Certify that they're conducting a lawful wiretap;

(3) Specify the source of the wiretap authority and its termination date; and

(4) Provide the chip ID number.

To provide greater reassurance, the certification by the DEA agents must be followed by a communication from a Federal government attorney associated with the matter, confirming that a wiretap has been lawfully authorized.

When the escrow agents receive a properly submitted request, they transmit their respective key components to the requesting agency; the components are combined within the decrypt processor which, only then, is able to decrypt communications using the particular chip. At the end of the authorized wiretap period, the decrypt processor's ability to decrypt communications using that particular chip will likewise terminate, and the escrow agents are to be so informed.

Those, in skeletal form, are the procedures for release of key components to Federal law enforcement agencies for criminal wiretaps. Similar procedures will apply to the release of key components for use in wiretaps authorized under State statutes. The most notable difference is that, for release to State or local law enforcement agencies, the request must come from the principal prosecuting attorney of the State or political subdivision involved—normally, the State Attorney General or the

District Attorney of the particular county. Finally, in the case of wiretaps under FISA, the request will be made by a Federal agency and will be subject to follow-up confirmation by the Department's Office of Intelligence Policy and Review.

The Administration recognizes that public confidence in this system is of paramount concern. The persons at NIST and Treasury who are responsible for the maintenance and, when appropriate, the release of key components are extremely serious about ensuring that they release key components only under proper circumstances. Meticulous procedures for the programming of the chips, and for the storage and handling of the keys, are being developed and refined. Even for tests of the system—decrypting communications over government-owned devices—there will be a full simulation of the request and release process.

The transactions of the escrow agents will be logged and recorded electronically, permitting subsequent review and audit. In addition, the Department of Justice will be responsible for ascertaining that the requesting agencies fully comply with the procedures at the various stages of the process. We will also reflect, in the respective reports to the Congress regarding wiretaps under Title III and FISA, those wiretaps in which key-escrow encryption was encountered and for which key components were released to a government agency.

Mr. Chairman, we have worked to develop procedures that strike the right balance between the rigorous protection of the privacy of communications and the need, in critical moments, to be able to decrypt such communications in order to protect lives and preserve the public safety. Through a combination of procedural requirements, technical safeguards, and audit capabilities, we believe that these procedures will assure the integrity of the key-escrow encryption system without frustrating the ability of government agencies to understand encrypted communications in the course of lawful wiretaps.

I have appreciated the opportunity to discuss with you this very important issue, and I shall be happy to try to answer any questions the Subcommittee may have.

Senator LEAHY. Thank you. I have a number of other questions for the record, but Senator Murray has joined us. She is proposing legislation on this, and before we go to Mr. Kammer, I didn't know, Senator, whether you had any questions you wanted to ask of Ms. Harris.

STATEMENT OF SENATOR PATTY MURRAY

Senator MURRAY. Well, thank you, Mr. Chairman. I will reserve my time to ask questions later. I do have an opening statement I will submit for the record. I very much appreciate your having this hearing and asking me to join you here today. This is an especially important topic in my State, where high technology is the key to our economic future and, really, the Clipper Chip proposal has had a chilling effect on a number of innovations that are coming along.

I have a number of questions that the chairman has asked that I think have not been satisfactorily answered. I believe that technology is going to be way ahead of where we are. I am very concerned that we are investing a great deal of time and energy and commitment into a Clipper Chip proposal, while our technology has moved way past that and it will be outdated within a very short time.

So, I will pass on questions at this time and will be here to hear the rest of the testimony. Thank you.

Senator LEAHY. Thank you.

[The prepared statement of Senator Patty Murray follows:]

PREPARED STATEMENT OF SENATOR PATTY MURRAY

Chairman Leahy, I appreciate the invitation to join you today for this important hearing.

Over the last decade, high technology and software manufacturing have become a strong force in Washington state's economy. Growth in this sector has helped off-

set job losses in aircraft manufacturing. Exports are an increasingly critical part of our software production, helping to cushion downturns in our domestic economy.

That is why the Administration's Clipper Chip proposal has had a chilling effect on software manufacturers in my state. For years, companies like Microsoft have struggled with burdensome, expensive and often anti-competitive U.S. export controls on encrypted software. Now, the Federal Government wants to dictate to companies what they can sell here at home, too.

High technology is key to our economic future. Cold War export controls are a thing of the past.

I have heard the arguments on all sides. On a laptop in my office in the Hart building, I have had DES encrypted software downloaded from Austria on the Internet. In January of this year, the Software Publishers Association found 210 foreign encryption products from 21 countries of which 129 use the Data Encryption Standard.

When I go with my teenagers to Egg head Software I read the "For Sale Only in the U.S." on Windows programs anyone can buy and pack in a suitcase. We cannot keep the genie in the bottle. The genie left a good long while ago, and Federal efforts to put the genie back in the bottle will be futile.

As the Acting Undersecretary of Commerce wrote to Banking Committee Chairman Riegle a few weeks ago: "At a time when product life cycles for high tech items last no longer than one or two years, the existing statute (the Export Administration Act) inhibits the long term market potential for U.S. industry." That is why I believe legislation I introduced with Senator Bennett in February, S. 1846, is the correct way to go on the export problem. My bill would retain controls on exports of generally available encrypted software for intelligence or military use, but not for commercial use.

I look forward to today's testimony.

Senator LEAHY. Mr. Kammer, it is all yours. Go ahead, and then we will go back to further questions.

STATEMENT OF RAYMOND G. KAMMER

Mr. KAMMER. Perhaps I could make three points and then go to the demonstration. First of all, the escrowed encryption standard is voluntary. It is not mandatory. It is voluntary for use both by government and by the private sector. Secondly—this is for the record because of some public discussion of this—there is no trap door in the escrow encryption standard. And then the third point is the U.S. Government needs encryption for civil privacy application—census data, the IRS, and the like.

Because the U.S. Government will ultimately buy a lot of whatever it selects, the price will presumably go down. Also, because people will have reasons to have conversations with the government perhaps in an encrypted environment, that will tend also to influence the marketplace. It seems to me that it is important that the government, to the extent it is influencing the marketplace, influence the marketplace in a way that does not harm law enforcement, and this standard does that.

Those are my three points. If you would like, I will go to a demonstration.

Senator LEAHY. Would you, please?

Mr. KAMMER. Sure. This is the TSD 3600 you have, Mr. Chairman, by you, and what I intend to do is phone you from here and then engage the TSD 3600, which has in it a Clipper Chip. What will happen is there will be an initial sort of negotiation between this device and the device there that will take about four seconds, and they are negotiating what is called a session key, which is a unique key that will engage the algorithm in the chip for our conversation, after which we will be able to have a conversation.

In addition, I have brought a tape recording of what people would hear if they intercepted because there wasn't any convenient way to set it up here.

Senator LEAHY. Sure.

Mr. KAMMER. So, with that, I will dial in.

Senator LEAHY. My God, it worked. I take back everything I said. [Laughter.]

Mr. KAMMER. We are now engaged in a normal encrypted conversation.

Senator LEAHY. I can hear it.

Mr. KAMMER. I will now engage the encryption. All you need to do is watch. At this point, the two devices are negotiating a session key. As I said before, it takes about four seconds. There is now emerged a session number which should be the same number for each of us, sir, which is FB 57.

Senator LEAHY. Interestingly enough, there is a slight delay, a fraction of a second delay, of the voices going back and forth. The only way I am aware of that is I can hear you in one ear, your actual voice, and hear you in here. But, obviously, it is being slowed down by about a quarter of a second.

Mr. KAMMER. Yes, sir. The quality of the voice, however—if we weren't in the same place, it would be a little less irritating. You can perceive the lag even if we were in remote locations, but the quality of the voice is actually quite good, in my opinion.

Senator LEAHY. Yes, it is very good, not like the old-fashioned scrambled phones.

Mr. KAMMER. With that, I have cleared and if you hit "clear" on your end, then we can just hang up. If there were now some person who was intercepting that conversation, or some other, it would sound as this will once I get it going.

[There follows a transcription of an audio tape:]

This recording is designed to demonstrate the ability of the TSD 3600, equipped with Clipper technology, to secure voice communications. I have been talking over a telephone with a TSD 3600 in the clear mode. I will now initiate the secure mode.

Senator LEAHY. That was the identifying number.

Mr. KAMMER. That is right. That was the preamble where they were negotiating a session key, and then that static sound is the white noise that people would hear.

Senator LEAHY. Now, has the Department of Justice bought these?

Mr. KAMMER. They have purchased 9,000 devices at this point.

Senator LEAHY. Is that going to replace the old STU phones?

Mr. KAMMER. The application that this is cleared for at this time is for civil data, not classified data. The STU's, as you know, are for classified data.

Senator LEAHY. Has anybody outside the government bought any of these devices with the Clipper Chip in it?

Mr. KAMMER. At this point, they are just coming on the market and if there are any deployed, it would be a negligible number at this point.

Senator LEAHY. And if I had this on my phone and you did not have it on yours, I can still call you just in the clear?

Mr. KAMMER. No problem; normal communications.

Senator LEAHY. But if I hit my red button, you are going to hear a beep and a clunk?

Mr. KAMMER. Well, it won't find anybody to negotiate with, so it will just sort of sit there and dither. [Laughter.]

Senator LEAHY. Heck, I am used to that. [Laughter.]

[The prepared statement of Raymond G. Kammer follows:]

PREPARED STATEMENT OF RAYMOND G. KAMMER

Introduction

Good morning. My name is Raymond G. Kammer, Deputy Director of the Commerce Department's National Institute of Standards and Technology (NIST). Thank you for inviting me here today to testify on the Administration's key escrow encryption initiative. The Computer Security Act of 1987 assigns NIST responsibility for the development of standards for protecting unclassified government computer systems, except those commonly known as "Warner Amendment systems" (as defined in Title 10 U.S.C. 2315).

In response to the topics in which the Committee expressed an interest, I would like to focus my remarks on the following:

(1) The principal encryption policy issue confronting us,

(2) The importance of encryption technology,

(3) How voluntary key escrow encryption technically works and how it ensures privacy and confidentiality,

(4) Alternatives to the voluntary key escrow initiative,

(5) Critical components of the Administration's policy on encryption technology,

(6) Recent initiative to modify Secure Hash Standard, and

(7) The effectiveness of the Computer Security Act of 1987.

1. THE PRINCIPAL ENCRYPTION POLICY ISSUE

First, I would like to broadly outline an important public policy and societal issue confronting us today regarding unclassified government and commercial cryptography. In developing cryptographic standards, one can not avoid two often competing interests. On the one hand are the needs of users—corporate, government, and individual—in protecting telecommunications transmissions of sensitive information. Cryptography can be used for excellent information protection. On the other hand are the interests of the national security and law enforcement communities in being able to monitor electronic communications. In particular, I am focusing upon their need for continued ability to keep our society safe from crime and our nation secure.

Rapid advances in digital telecommunications have brought this issue to a head. Some experts have stated that, within ten years, most digital telecommunications will be encrypted. Unless we address this issue expeditiously, law enforcement will lose an important tool in fighting crime—the ability to wiretap—and the mission of our Intelligence Community will be made more difficult. The Committee is undoubtedly aware of the benefits such intelligence brings to the nation. This matter raises broad societal issues of significant importance. I have personally been involved in many meetings of a philosophical and wide-ranging nature to discuss this dilemma.

Four broad conceptual alternatives emerged:

- Seek a legislative mandate criminalizing the use of unauthorized cryptography.
- Seek wide adoption of an encryption method with an unannounced "trap door." This was never seriously considered.
- Seek wide voluntary adoption of a technology incorporating a secure "key escrow" scheme.
- Allow technology to evolve without government intervention; in effect, do nothing.

None of these options satisfies all interested parties fully. I doubt such a solution even exists, but the Administration has chosen the voluntary key escrow technology approach as the most desirable alternative for protecting voice communications without impairing the ability of law enforcement agencies to continue to conduct wiretaps. For data communication the long-standing Data Encryption Standard has recently been recertified for use.

It is interesting to note that other countries have faced this same issue and chosen different solutions. France, for example, outlaws the use of unregistered cryptographic devices within its borders.

2. THE IMPORTANCE OF ENCRYPTION TECHNOLOGY

Encryption provides one of the best ways to guarantee information integrity and obtain cost-effective information confidentiality. Encryption transforms intelligible information into an unintelligible form. This is accomplished by using a mathematical algorithm and a "key" (or keys) to manipulate the data in a complex manner. The resulting enciphered data can then be transmitted without fear of disclosure, provided, of course, that the implementation is secure and the mathematical-based algorithm is sound. The original information can then be understood through a decryption process. As I shall discuss, knowledge of the particular key utilized for a particular encryption of information (or, in the case of asymmetric cryptography, knowledge of the associated key of the key pair) allows decryption of the information. For this reason, such keys are highly protected.

Uses of cryptography

Encryption can be used in many applications for assuring integrity and confidentiality, or both. It can be used to protect the integrity and/or confidentiality of phone calls, computer files, electronic mail, electronic medical records, tax records, corporate proprietary data, credit records, fax transmissions and many other types of electronic information. It is expected that cryptographic technologies will be used on a voluntary basis in the protection of information and services provided via the National Information Infrastructure.

Encryption used with these and other types of information protects the individual privacy of our citizens including, for example, their records and transactions with government agencies and financial institutions. Private sector organizations can also benefit from encryption by securing their product development and marketing plans, for example. It also can protect against industrial espionage by making computers more secure against unauthorized break-ins and, if data is encrypted, making it useless for those without the necessary key.

The government has long used cryptography for the protection of its information—from that involving highly classified defense and foreign relations activities to unclassified records, such as those protected under the Privacy Act. My point here is not to list all potential applications and benefits but to give you a feel for the innumerable applications and benefits which encryption, when securely implemented, can provide.

Hazards of cryptography

Counterbalanced against its benefits, encryption also can present many substantial drawbacks—to both the government and other users. First and foremost, encryption can frustrate legally authorized criminal investigations by the federal, state, and local law enforcement agencies. As their representatives can better explain, lawful electronic surveillance has proven to be of the utmost benefit in both investigating and prosecuting serious criminal activity, including violent crime. Cryptographic technologies can also seriously harm our national security and intelligence capabilities. As I shall discuss, the Administration recognizes that the consequences of wide-spread, high quality encryption upon law enforcement and national security are considerable.

Encryption may also prove a potential hazard to other users, such as private sector firms, particularly as we move into the Information Age. Private firms, too, are concerned about the misuses of cryptography by their employees. For example, a rogue employee may encrypt files and offer the "key" for ransom. This is often referred to as the "data hostage" issue. Keys can also be lost or forgotten, resulting in the unavailability of data. Additionally, users of encryption may gain a false sense of security by using poorly designed or implemented encryption. To protect against such hazards, some corporations have expressed interest in a "corporate" key escrowing capability to minimize harm to their organizations from internal misuse of cryptography. As security experts point out, such a false sense of security can be worse than if no security measures were taken at all. Encryption is not a "cure-all" to all security problems.

Let me now turn to the details of the Administration's key escrow encryption initiative.

3. VOLUNTARY KEY ESCROW ENCRYPTION INITIATIVE

Goals of the voluntary key escrow encryption initiative

I will begin my remarks about the government-developed key escrow encryption chips (referred to as "chips" herein) by discussing the goals that we were trying to achieve in developing this technology for application to voice-grade communication.

At the outset, we sought to develop a technology which provides very strong protection for government information requiring confidentiality protection. Much of the sensitive information which the government holds, processes, and transmits is personal and requires strong protection. Tax records and census data are two such examples. We sought nothing less than excellent protection for government communications. In order to allow agencies to easily take advantage of this technology, its voluntary use (in Federal Information Processing Standards (FIPS) 185) to protect telephone communications has been approved by the Secretary of Commerce.

The chips implementing FIPS 185 efficiently support applications within its scope. They far exceed the speed requirements of commercial modems existing today or envisioned for the near future.

In addition to the need for strong information protection, the increasingly digitized nature of advanced telecommunications is expected to significantly hamper the ability of domestic law enforcement to carry out lawfully authorized wiretapping. Their problem has two dimensions.

First, the design and complexity of the nation's telecommunications networks makes locating those communications which can be lawfully tapped very difficult. This is the digital telephony issue, which my law enforcement colleague will discuss today.

Second, the proliferation of encryption is expected to make law enforcement's tasks more difficult. If a telephone conversation is encrypted, resources must be expended for decryption, where feasible. Such expenditures and technical capabilities are normally far outside the ability of local law enforcement organizations and could be quite significant at the federal level. In seeking to make available a strong encryption technology, we have sought to take into account the needs of the law enforcement community. For example, one of the reasons that the SKIPJACK algorithm, the formula on which the key escrow chip is based, is being kept classified is that its release would make their job much harder were it to be used to hide criminal activity.

Misconceptions concerning the purpose of the voluntary key escrow encryption initiative

A number of those opposed to this Administration initiative have expressed doubt about whether the key escrow encryption initiative can do anything to solve this nation's crime problem. Of course, this initiative cannot by itself do so. The basic intent of the program is the provision of sound security, without adversely affecting other government interests, including, when necessary, the protection of society through lawfully authorized electronic surveillance.

The voluntary key escrow encryption initiative, first and foremost, was devised to provide solid, first-rate cryptographic security for the protection of information held by the government when government agencies decide such protection is needed for unclassified government communications—for example, tax, social security and proprietary information (The Escrowed Encryption Standard (FIPS 185) allows federal agencies to use this technology for protection of telephone communications.) This was done, in part, with the realization that the current government cryptographic technique, the Data Encryption Standard (which was recently re-approved) is over fifteen years old; while DES is still sound, its usefulness will not continue indefinitely. We also recognized that were we to disclose an even stronger algorithm (with the government's "seal of approval"), it could be misused to hamper lawful investigations, particularly electronic surveillance.

In approving this initiative, we felt it important that protective measures be taken to prevent its misuse—a safety catch, if you will. This will help assure that this powerful technology is not misused if adopted and used voluntarily by others. Our method of providing this safety mechanism relies upon escrowing cryptographic key components so that, if the technology is misused, lawful investigations will not be thwarted. Additionally, the algorithm (SKIPJACK) will remain classified so that its only uses will be consistent with our safety mechanism, key escrowing. I think it is fair to say that use of this powerful algorithm without key escrowing could pose a serious threat to our public safety and our national security.

Key escrow encryption technology

The National Security Agency, in consultation with NIST and the federal law enforcement community, undertook to apply voluntary key escrow encryption technology to voice-grade communications. The product of this effort was announced in the April 16, 1993 White House release concerning the key escrow encryption chip. I note that we have chosen to discontinue use of the term "Clipper Chip" to avoid potential confusion with products and services with similar names.

The state-of-the-art microcircuit, the key escrow encryption chip, can be used in new, relatively inexpensive encryption devices that can be attached to an ordinary telephone. It scrambles telephone communications using an encryption algorithm more powerful than many in commercial use today. The SKIPJACK algorithm, with an 8-bit long cryptographic key, is approximately 16 million times stronger than DES. For the record, I will restate my earlier public statements that there is no trapdoor in the algorithm.

Each key escrow encryption chip has two basic functions. The first is an encryption function, which is accomplished by the SKIPJACK algorithm, developed and rigorously tested by NSA. The second function is a law enforcement access method. I will discuss each briefly.

The SKIPJACK algorithm is a symmetric algorithm (as opposed to "public-key" algorithms). Basically, this means that the same cryptographic key (the session key) is used for both encryption and decryption. The algorithm is so strong that the Department of Defense will evaluate it for use in protecting selected classified applications.

The second basic function of the chip is the provision for law enforcement access under lawful authorization. To do so, each chip is programmed with three values: a cryptographic family key, a device unique key, and a serial number. (The device unique key is split into two key components which are then encrypted and are provided to the two current escrow agents, NIST and the Automated Systems Division of the Department of the Treasury, for secure storage.) These three values are used in conjunction with the session key (which itself encrypts the message) in the creation of the law enforcement access field. When law enforcement has obtained lawful authorization for electronic surveillance, the serial number can be obtained electronically. Law enforcement can then take the serial number and a certification of their legal authorization to the two escrow agents. (Detailed procedures for the release of these key components were issued by the Department of Justice in early February.) After these certifications are received, the encrypted components will be transmitted by escrow agent officials for combination in the decrypt-processor.

After decryption of the key components within the decrypt processor, the two key components are then mathematically combined, yielding the device unique key. This key is used to obtain another key, the session key, which is used to decrypt and understand the message. This device unique key may be used by law enforcement only for the decryption of communications obtained during the applicable period of time of the lawful electronic surveillance authorization. It can also only be used to decrypt communications transmitted or received by the device in question.

Security and privacy using key escrow encryption

When the Administration announced the voluntary key escrow encryption initiative, we anticipated that questions would be raised about the strength and integrity of the SKIPJACK algorithm, which is at the heart of the system. We assured the public that we knew of no weakness in the algorithm and that there was not an undisclosed point of entry, commonly referred to as a trapdoor. The algorithm was designed by cryptographic experts at the National Security Agency and withstood a rigorous testing and analysis process.

As a further way to indicate the fundamental strength of SKIPJACK, we invited a group of independent experts in cryptography to review the algorithm, under appropriate security conditions, and make their results publicly known, again, consistent with the classified nature of the algorithm. This group consisted of Ernest Brickell (Sandia National laboratories), Dorothy Denning (Georgetown University), Stephen Kent (BBN Communications Corp.), David Maher (AT&T) and Walter Tuchman (Amperif Corp.). These experts reported that:

- Under an assumption that the cost of processing power is halved every eighteen months, it will be 36 years before the cost of breaking SKIPJACK by exhaustive search will be equal to the cost of breaking DES today;

and

- There is no significant risk that SKIPJACK can be broken through a shortcut method of attack.

Let me also repeat the reasons why the algorithm must remain classified. First, we believe it would be irresponsible to publish the technical details. This would be tantamount to handing over this strong algorithm to those who may use it to hide criminal activity. Publishing the algorithm may also reveal some of the classified design techniques that NSA uses to design military-strength technology. It would also allow devices to be built without the key escrowing feature, again allowing criminals to take advantage of the strength of this very powerful technology without any safeguard for society.

With regard to privacy, key escrow encryption can, of course, be used to protect personal information contained in telephone communications. Moreover, the voluntary key escrow encryption initiative does not expand the government's authority for the conduct of electronic surveillance, as my colleague from the Federal Bureau of Investigation will discuss. It is important to understand that the escrow agents will not track the devices by individual owners; they will simply maintain a database of chip ID numbers and associated chip unique key components (which themselves are encrypted).

4. ALTERNATIVES TO THE VOLUNTARY KEY ESCROW INITIATIVE

In reaction to industry's concerns about our hardware-only implementation of key escrow encryption, we announced an opportunity for industry to work with us on developing secure software-based key escrow encryption. Unfortunately, initial industry interest was minimal; our offer, however, remains open. We are also willing to work on hardware alternatives to key escrowing as we emphasized in our recent announcements.

The Administration has been seeking to meet with members of the computer, software, and telecommunications industries to discuss the importance of this matter. We are open to other approaches.

5. KEY GOVERNMENT POLICIES ON UNCLASSIFIED/COMMERCIAL ENCRYPTION

Encryption is an important tool to protect privacy and confidentiality

As I discussed earlier, encryption is powerful technology that can protect the confidentiality of data and the privacy of individuals. The government will continue to rely on this technology to protect its secrets as well as the personal and proprietary data it maintains. Use of encryption by federal agencies is encouraged when it cost-effectively meets their security requirements.

No legislation restricting domestic use of cryptography

Early in the policy review process, we stated that the Administration would not be seeking legislation to restrict the use, manufacture, or sale of encryption products in the U.S. This was a fear that was expressed in the public comments we received, and one that continues, despite our repeated assertions to the contrary. Let me be clear—this Administration does not seek legislation to prohibit or in any way restrict the domestic use of cryptography.

Export controls on encryption are necessary but administrative procedures can be streamlined

Encryption use worldwide affects our national security. While this matter cannot be discussed in detail publicly without harm to this nation's intelligence sources and methods, I can point to the Vice President's public statement that encryption has "huge strategic value." The Vice President's description of the critical importance of encryption is important to bear in mind as we discuss these issues today.

In recent months, the Administration has dramatically relaxed export controls on computer and telecommunications equipment. However, we have retained export controls on encryption technology, in both hardware and software. These controls strongly promote our national security. These export controls include mass market software implementing the Data Encryption Standard. The Administration determined, however, that there are a number of reforms the government can implement to reduce the burden of these controls on U.S. industry.

These reforms are part of the Administration's goal to eliminate unnecessary controls and ensure efficient implementation of those controls that must remain. For example, fewer licenses will be required by exporters since manufacturers will be able to ship their approved products from the U.S. directly to customers within approved regions without obtaining individual licenses for each end user. Additionally, the State Department has set a license review turnaround goal of two working days for most applications. Moreover, the State Department will no longer require that U.S. citizens obtain an export license prior to taking encryption products out of the U.S. temporarily for their own personal use. Lastly, after a one-time initial technical

review, key escrow encryption products may now be exported to most end users. These reforms should help to minimize the effect of export controls on U.S. industry.

The government requires a mechanism to deal with continuing encryption policy issues

In recognition of this, the Interagency Working Group on Encryption and Telecommunications was formed in recognition of the possibility that the economic significance of our current encryption policy could change. The Working Group has been assigned to monitor changes in the balance that the President has struck with these policy decisions and to recommend changes in policy as circumstances warrant. The Working Group will work with industry on technologies like the key escrow encryption chip and in the development and evaluation of possible alternatives to the chip.

The group is co-chaired by the White House Office of Science and Technology Policy and the National Security Council. It includes representatives from all departments and agencies which participated in the policy review and others as appropriate, and keeps the Information Policy Committee of the Information Infrastructure Task Force apprised of its activities.

Flexibility on encryption approaches

From the time of the initial White House announcement of this technology, we have stated that this key escrow encryption technology provides:

(1) Exceptionally strong protection and

(2) A feature to protect society against those that would seek to misuse it.

I have personally expressed our flexibility in seeking solutions to these difficult issues. We have offered to work with industry in developing alternative software and hardware approaches to key escrowing. We actively seek additional solutions to these difficult problems.

We also stand willing to assist the Congressionally-directed study of these issues by the National Research Council.

Use of EES is voluntary and limited to telephone systems

The Escrowed Encryption Standard, which was approved on February 3, 1994, is a voluntary standard for use both within and outside of the federal government. It is applicable for protecting telephone communications, including voice, fax and modem. No decisions have been made about applying key escrow encryption technology to computer-to-computer communications (e.g., e-mail) for the federal-government.

Government standards should not harm law enforcement/national security

This is fairly straightforward, but can be difficult to achieve. In setting standards, the interests of all the components of the government should be taken into account. In the case of encryption, this means not only the user community, but also the law enforcement and national security communities, particularly since standards setting activities can have long-term impacts (which, unfortunately, can sometimes be hard to forecast).

6. SECURE HASH STANDARD

As the Committee may be aware, NIST has recently initiated the process to issue a technical modification to Federal Information Processing Standard 180, the Secure Hash Standard. The Secure Hash Standard uses a cryptographic-type algorithm to produce a short hash value (also known as a "representation" or "message digest") of a longer message or file. This hash value is calculated such that any change to the file or message being hashed, will, to a very high degree of probability, change the hash value. This standard can be used alone to protect the integrity of data files against inadvertent modification. When used in conjunction with a digital signature, it can be used to detect any unauthorized modification to data.

Our intent to modify the standard was announced by NIST after the National Security Agency informed me that their mathematicians had discovered a previously unknown weakness in the algorithm. This meant that the standard, while still very strong, was not as robust as we had originally intended. This correction will return the standard to its intended level of strength.

I think this announcement illustrates two useful issues with regard to cryptographic-based standards. First, developing sound cryptographic technology is very difficult. This is also seen with commercial algorithms, including those used for hashing and encryption. Secondly, this incident demonstrates the commitment of

NIST, with NSA's technical assistance, to promulgating sound security standards. In this case, a weakness was found, and is being quickly corrected.

7. EFFECTIVENESS OF THE COMPUTER SECURITY ACT OF 1987

Lastly, as requested in your invitation to appear here today, let me briefly address the effectiveness of the Computer Security Act of 1987 (P.L. 100–235). I will first briefly comment on what we learned about the state of computer security in the federal government during our agency visit process and then turn to cryptographic-specific issues.

As part of our efforts to increase awareness of the need for computer security, during 1991–1992, officials from OMB, NIST and NSA visited 28 federal departments and agencies. Each visit was designed to increase senior managers' awareness of security issues and to motivate them to improve security. I believe that what we learned during those visits remains valid—and indicates that we still need to focus on basic computer security issues in the government.

Specifically, OMB, NIST and NSA proposed the following steps to improve security:

- Focus management attention on computer security.
- Improve planning for security.
- Update security awareness and training programs.
- Improve contingency planning and incident response capabilities.
- Improve communication of useful security techniques.
- Assess security vulnerabilities in emerging information technologies.

Actions are being taken by NIST and other agencies to address each of these areas. The background and discussion of the need for these measures is discussed in the summary report prepared by OMB on "Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90–08" (February 1993). In short, the Computer Security Act provides an appropriate framework for agencies—to continue improving the security of their automated systems—but much work remains to be done, by NIST and individual federal agencies.

One of the questions that the Committee was interested in was whether there is a need to modify this legislation in response to the same advancements in technology that led to the key escrow initiative and digital telephony proposal. First, I would observe that the Act, as a broad framework, is not tied to a specific technology. I think it would be unworkable if the Act were to address specific computer technologies, since this is a rapidly evolving field. Also, I would note that the Act does not address digital telephony concerns—the Administration is proposing separate legislation in that area. In short, no modifications to the Act are necessary because of technology advances.

Before leaving the subject of the Computer Security Act, however, let me briefly comment on the Escrowed Encryption Standard. I strongly believe that NIST and NSA have complied with the spirit and intent of the Act. At the same time, this issue underscores the complex issues which arise in the course of developing computer security standards, particularly cryptographic-based standards for unclassified systems.

The Act, as you are aware, authorizes NIST to draw upon computer security guidelines developed by NSA to the extent that NIST determines they are consistent with the requirements for protecting sensitive information in federal computer systems. In the area of cryptography, we believe that federal agencies have valid requirements for access to strong encryption (and other cryptographic-related standards) for the protection of their information. We were also aware of other requirements of the law enforcement and national security community. Since NSA is considered to have the world's foremost cryptographic capabilities, it only makes sense (from both a technological and economic point of view) to draw upon their guidelines and skills as useful inputs to the development of standards. The use of NSA-designed and -tested algorithms is fully consistent with the Act. We also work jointly with NSA in many other areas, including the development of criteria for the security evaluation of computer systems. They have had more experience than anyone else in such evaluations. As in the case of cryptography, this is an area in which NIST can benefit from NSA's expertise.

Summary

Key escrow encryption can help protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted telephonically. Key escrow encryption is available as a valuable tool for

protecting federal agencies' critical information communicated by telephone. At the same time, this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

Encryption technology will play an increasingly important security role in future computer applications. Its use for security must be balanced with the need to protect all Americans from those who break the law.

Thank you, Mr. Chairman. I would be pleased to answer your questions.

Raymond G. Kammer is the Deputy Director of NIST. He is responsible for the day to day operation of the Institute as well as long-range planning and policy development. NIST is the only Federal laboratory explicitly charged with providing technical research and services to enhance U.S. industrial competitiveness. NIST provides support for industry's development of precompetitive generic technologies and diffusing technological advances to users in all segments of the economy. In addition, NIST provides the measurements, calibrations, and quality assurance techniques which underpin U.S. commerce, technological progress, improved product reliability and manufacturing processes, and public safety. NIST carries out many of these efforts in partnership with industry and government.

A graduate of the University of Maryland, Kammer joined NIST in 1969 as a program analyst. Over the following decade he served the agency and the U.S. Department of Commerce in a succession of offices concerned with budgetary and program analysis; planning; and personnel management. In 1980, Mr. Kammer was appointed Deputy Director of NIST. He also has served as Acting Director of NIST, Acting Director of the National Measurement Laboratory, and Acting Director of the Advanced Technology Program.

In 1991, Kammer was named the Deputy Under Secretary for Oceans and Atmosphere, NOAA, Department of Commerce. While in that position, he served as NOAA's Chief Operating Officer and was responsible for overseeing the day-to-day operation of NOAA's five major line offices. In 1993, Kammer returned to NIST as Deputy Director.

In addition, Kammer has chaired several important evaluation committees for the Department of Commerce, including reviews of satellite systems for weather monitoring and the U.S. LANDSAT program, and the next generation of weather radars used by the U.S. government. He also served a three-year term on the Board of Directors of ASTM, a major international government for the development of voluntary standards for materials, products, systems, and services.

His awards include both the Gold and Silver medals of the Department of Commerce, the William A. Jump Award for Exceptional Achievement in Public Administration, the Federal Government Meritorious Executive Award, and the Roger W. Jones Award for Executive Leadership.

Senator LEAHY. You are working with industry, as I understand it, to improve on the key escrow chips, to develop key escrow software, and to examine alternatives to Clipper Chip. What are the improvements and alternatives to Clipper Chip that NIST is considering, or have I overstated the situation?

Mr. KAMMER. We are in active collaboration with four private sector entities that responded to a public advertisement that we made, and the intent was to have discussions both on hardware improvements and software. In the case of the hardware improvements, what people are interested in is can the algorithm be incorporated on some other chip that is already in a communications device, for instance, thereby reducing the power requirements.

The full name of the game in communications is you want to be portable, you want to be light, you want to take no power at all, ideally, or very little power. To incorporate the clipper hardware on a portable telephone, for instance, it uses enough power now to be irritating to the manufacturers. They don't think it is very attractive until we can reduce the power.

In terms of the software, we would like to see if we can find a concept, and we have not yet, where we would be able to preserve law enforcement and still encrypt in a software mode rather than

a hardware mode. Intellectually, that is a very formidable idea. If you could ever think of a way of doing it, you would have the best of all worlds, in that you use no power when you use software and, of course, it doesn't weigh anything, so that would be very desirable.

Those discussions have been—the group that has been undertaking this has been meeting biweekly since last—bimonthly—I am sorry—since last December working on these issues.

Senator LEAHY. There is no way to get in on the conversation you and I had? There would be no way for somebody to put a device like this on the line between the two of us and pick it up, or is there?

Mr. KAMMER. Yes, sir, there would be, with considerable effort. I mean, they would have to know which line it was going to pass through, which is a very formidable problem in itself, but let us say somehow people have——

Senator LEAHY. Well, let us say you are calling me from Chicago and I am in Vermont, but they know what office you are going to call from.

Mr. KAMMER. Right, so they would put it on a wire.

Senator LEAHY. So they would have to be within a few feet of where you are. Can they do that?

Mr. KAMMER. Then what would happen is you would not get the indication that it was secure. The negotiation would say "retry" instead of "secure."

Senator LEAHY. It would pick up the fact that there is something in the way of the connection?

Mr. KAMMER. It would know that there was what we call a man in the middle. It would know that there is such an individual there. If I went to that much trouble, probably what I would rather do is just put a microphone under your desk.

Senator LEAHY. Well, that was going to be my next question.

The National Research Council of the National Academy of Sciences is doing a 2-year study of shortcomings in how national encryption policy is made, and Clipper Chip, and so on. Is there any reason why the administration couldn't wait to implement its Key Escrow Encryption System until after we got this study?

Mr. KAMMER. The urgency from our point of view was that products like the TSD 3600 were coming into the marketplace, and what drove us was indeed that happening and the possibility—and this can still happen, but the technology would just whirl ahead of us and we would wake up one morning—suddenly there were fax machines everywhere, you know, and maybe suddenly there was the TSD 3600 with an algorithm in it that was very vexing to law enforcement, and that could still happen. I mean, Clipper is voluntary. People could pick something else, and they may.

Senator LEAHY. Well, suppose they don't pick Clipper Chip. Are we going to stop the use of it?

Mr. KAMMER. No, sir. We still have a substantial influence on the marketplace just because of price and because of the convenience of communicating with the government. Additionally, the experts in this field, I think, tend to underestimate the formidable task of most normal people setting up their own personal encryption net. It is not a trivial thing to do.

Indeed, many people use good algorithms and set the net up so poorly that they are exploitable because of the defects in how they set it up. In a nation where most people can't program their own VCR's, I mean this is something to think about.

Senator LEAHY. Senator Murray points out it is OK because our kids can. There is an 8-year-old girl who lives across the street and we call her over to set the thing up and she takes care of it for us. [Laughter.]

Are foreign governments going to permit the use of Clipper Chip or Capstone overseas?

Mr. KAMMER. We have started some discussions with foreign governments. It is an interesting problem. Most of the Western European countries actually have laws on the books, in many cases since the 1920's, that allow them to regulate all use of encryption. Some countries are rather active in their enforcement of these laws, some are rather lax, but the laws exist on the books.

Senator LEAHY. If we are setting an industry standard, what do you do if some of the major countries, especially those that have major commercial interests with us, say no, or we will let you use it, but only if we have the keys?

Mr. KAMMER. That is all a negotiation to take place.

Senator LEAHY. Is any of it taking place now?

Mr. KAMMER. There have been some initial discussions with selected governments. It may be that Admiral McConnell would have more to share with you in the following session.

Senator LEAHY. Now, I understand that software is available that could be used with Clipper to bypass the key escrow feature. A sender of information can first encrypt the information with software using DES or RSA algorithms, then transmit that information double-encrypted with Clipper. So, in other words, even if you decrypt Clipper, what you do is you peel the onion off and underneath it is still an onion, an encrypted one. Doesn't that defeat you?

Mr. KAMMER. You are exactly correct, and indeed that would confound our intent. However, you had to go through a couple of troublesome steps here and to the extent that you have done it successfully, we are confounded. Most people probably won't go to that much trouble, experience suggests, or won't do it successfully, experience suggests.

Senator LEAHY. Is the administration considering outlawing all other encryption methods?

Mr. KAMMER. We took as one of our assignments during the presidentially instructed review to consider that and we rejected it. We think that mandatory regulation in this area would be an inappropriate approach for our society.

Senator LEAHY. Last year when you testified before Representative Markey's subcommittee, you were asked if foreign companies would purchase Clipper Chip and you replied, "I think under the current circumstances, probably if I were running a foreign company, that would be a decision I would not make." Do you still feel that way?

Mr. KAMMER. I have been surprised. In conversations with a lot of the multinational companies, what they seem to assign a very high priority to is something they can use everywhere. They are

substantially less concerned about the ability of our government, at least, to access their information. They have expressed concerns about what they view as the practice of some other governments of intercepting commercial information to share with commercial companies, and that does worry them, but people were less resistant than I imagined at that time.

Senator LEAHY. So if you were back there last April before Congressman Markey's subcommittee, would you give the same answer?

Mr. KAMMER. Knowing what I knew then, I think I would have been obliged to.

Senator LEAHY. No, but today.

Mr. KAMMER. No, I wouldn't.

Senator LEAHY. If other countries don't let Clipper Chip in, do we have a problem using the information superhighway that everybody wants to get on now? I mean, I look at Internet where I can go and pick up articles from a university in Australia or communicate with somebody in Eastern Europe. I mean, what about this? Are we suddenly going to see countries cutting off Internet?

Mr. KAMMER. There is going to have to be at some point a worldwide solution to this. The power of Internet is too attractive. People aren't going to be willing to forgo that, and any country that forgoes is forgoing economic opportunity that means they won't survive for that long.

The critical things that you are going to need for commerce are, first of all, digital signature. If you want to sell or buy from people you have never met, you have to have some unambiguous way of assuring that they indeed incurred the debt and that they are liable for it. Digital signature is that solution. You are going to need some way of sealing data so you can be confident that it wasn't changed. That is sometimes called message authentication. Those two things are absolutely necessary for commerce. For many kinds of commerce, you are also going to need some kind of confidentiality that goes across borders. This is a difficult problem.

Senator LEAHY. And it becomes more difficult if Clipper Chip is the standard. I really cannot imagine a number of these countries allowing it, no matter what commercial disadvantage they might be put at, without having a way of cracking into it.

Mr. KAMMER. The possibility of some solution that doesn't involve a trusted third party, whoever it is—I haven't thought of anything myself, nor have I talked to anybody that has thought of anything that goes to some balance between protection from criminal activities balanced with privacy. What most people say it is not possible to do it at all and therefore let us just go a hundred percent privacy, the heck with the law enforcement. I don't know how it is going to come out.

Senator LEAHY. Well, can you imagine any groundswell of enthusiasm here in the United States for giving these keys to some other country, no matter who they are?

Mr. KAMMER. I can't.

Senator LEAHY. Now, I understand that the cost of establishing the escrow system will be about $14 million and the cost of running it will be about $16 million annually. Is there any statutory authority for these expenditures?

Mr. KAMMER. During the review that we did, there was a legislative review as well and we have the authority under the Computer Security Act, as it amended the NIST Organic Act. There is no authorization for the money at this point.

Senator LEAHY. Ms. Harris, I think you were very forthcoming with the Justice Department's view on legislation, but if there is enough concern here, there will be legislation.

Senator Specter?

Senator SPECTER. Thank you very much, Mr. Chairman.

In noting the examples of cryptographic products which are being produced by others, are there some, Mr. Kammer, that are more complicated and more difficult to decrypt?

Mr. KAMMER. If you have two well-designed algorithms, then the measurement is usually something called the work factor, and that is how long it would take you to try all the possible keys that exist, but that first big "if" is a real big "if." There are algorithms that are out in public use that seem to have rated very long work factors that indeed are not all that well designed. So, first, you have to know is it really designed as well as it is labeled, and then, secondly, if so, then you can start comparing work factors. Presuming two good algorithms, the one with the biggest work factor is presumably the best one.

Senator SPECTER. Well, you lost me. Let me try again.

Mr. KAMMER. Sure.

Senator SPECTER. Are there some cryptogram systems that we cannot break at this moment?

Mr. KAMMER. Yes, sir.

Senator SPECTER. Are there any cryptogram systems that cannot be broken with enough energy and time applied?

Mr. KAMMER. No, sir, but the amount of time could range into hundreds, you know, of years.

Senator SPECTER. All right, so criminal elements or foreign agents could have access to cryptogram systems which we might not be able to break except with very extensive efforts.

Mr. KAMMER. That is correct. That presumes a rather sophisticated criminal who is also very disciplined about implementing the system, but yes.

Senator SPECTER. General Harris, what pause does that give you for wiretaps if it is possible for organized crime or sophisticated foreign agents to use these cryptographic systems?

Ms. HARRIS. It is clearly of grave concern. Our hope with Clipper Chip is that it will become a device of choice so widespread that at least we will not have developed and then made available privately a technology which will frustrate law enforcement.

Senator SPECTER. With so many of these other cryptographic devices available from so many other countries—Australia, Denmark, Finland, Germany, Israel, Russia, the United Kingdom—isn't there sufficient competition with this kind of a device so that whatever we do with ours won't make a whole lot of difference? Won't foreign agents or criminals who want access to secret cryptography will be able to have it, whatever we do with Clipper Chip?

Ms. HARRIS. It is our hope that if Clipper Chip becomes the standard of choice for legitimate businesses that there will come a

time when even illegitimate criminal enterprises will have to communicate with legitimate operators around the world.

Senator SPECTER. But, General Harris, why should it become the product of choice when there are so many others available?

Ms. HARRIS. I must tell you, Senator, that my understanding is that although others are available, they are not that good; that Clipper is—probably "light years" is strong a word, but that Clipper is so much stronger than the available—is so much stronger and so much better than what is available that, developed and made available, as the intention is, to the market, it will be the encrypter of choice. I mean, that is the hope. At least it will be one that this country has developed which will not frustrate law enforcement.

Senator SPECTER. Given technology's rapid advances, is there any estimate as to how long it would be before someone is likely to produce a better system?

Ms. HARRIS. I think that I would not speculate on that, Senator. Clearly, people are working on it, and clearly we are not just sort of stopped with Clipper Chip either. I mean, there must be a continuing review and work on this subject. I mean, this is a subject of grave concern to law enforcement, I am sure you understand.

Senator SPECTER. When the codes would be in the hands of two governmental agencies, is there a possibility that they might be used without a court order in a system which requires a court order for a wiretap?

Ms. HARRIS. I do not believe that they will be misused without court order. We have built into our protocols several fail-safe provisions. For instance, as you have noted, first of all, obviously, we have got to have a court order. The certification by the law enforcement agent who picks up an encoded conversation pursuant to Clipper Chip is required to certify to both of the independent key escrow holders that there is a court order, when it is going to end, and the identifying numbers.

Each one of those independent escrow agents has to act independently to send back to the decrypt device the appropriate codes that have to be combined in the machine, and then the responsible Federal officer, if it is a Federal wiretap——

Senator SPECTER. Who is the custodian for this code in the Department of Justice, or who is the proposed custodian?

Ms. HARRIS. For the two escrow agents?

Senator SPECTER. Yes.

Ms. HARRIS. NIST is one, and what comes down to the command center at the Department of Treasury is the other right now.

Senator SPECTER. So Justice will not be a custodian?

Ms. HARRIS. That is absolutely correct. We have very carefully picked key escrow holders that are not law enforcement agencies.

Senator SPECTER. Treasury has significant law enforcement functions.

Ms. HARRIS. Not this aspect of Treasury, Senator.

Senator SPECTER. Which aspect is it?

Ms. HARRIS. It comes down to the command center at Treasury. It is part of their Automated Systems Division. It is on their administrative side.

Senator SPECTER. Well, it is very interesting. I recall being a lieutenant in the Air Force years ago in the Office of Special Investigation in the special branch called Cryptography, and from that vantage point I have always doubted that anything is a secret.

I have had experience where only three highly trusted people in a major investigation I ran years ago in the district attorney's office in Philadelphia knew about a matter; I have always had real reservations about how secret you can be.

Let me just ask both of you one final question, and that is do you really think we can make it so that it is secret? General Harris?

Ms. HARRIS. I believe that we can make it and, with human and mechanical technological safeguards, make it literally impossible for the whole system to be misused, and that it will function pursuant to court-authorized interceptions and function simply as a translator, so to speak, so that we can understand the content of communications that a court has authorized us to intercept.

Senator SPECTER. Mr. Kammer, will it really be secret?

Mr. KAMMER. Yes, sir, I believe that we can be successful in making it secret.

Senator SPECTER. Well, the technology is fascinating. We had the Director of the FBI in on a hearing not too long ago and the shoe was on the other foot. The Director of the FBI was asking for legislation which would enable the FBI to keep up with the crooks, with all of the changes in the telephone system. So this subcommittee has its work cut out for it, but we will try to be helpful.

Thank you very much. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Murray?

Senator MURRAY. Thank you, Mr. Chairman.

Mr. Kammer, has NIST evaluated the foreign programs that are available?

Mr. KAMMER. We have occasionally evaluated selected ones out of interest. The NSA has done a much more thorough-going job and you may find it useful to discuss that in the next hearing.

Senator MURRAY. OK; thank you. On April 28, the Wall Street Journal quoted a computer expert as predicting criminals will routinely encrypt information within 2 years. Do you agree with that assessment?

Mr. KAMMER. I think the timeframe of 2 years is extremely unlikely at this point. I don't think there will be widespread use even among sophisticated users in 2 years.

Senator MURRAY. Would Clipper Chip affect that timetable in any way?

Mr. KAMMER. Well, I can sort of reason by analogy. DES was released 17 years ago and for the first 5 years it was regarded, because it had come from the government, with fear and loathing by all, and then it gradually began to penetrate the marketplace and now it is the choice for banking and for a number of other uses. That process took about 12, 13 years before it really got to the point where it was in widespread use. I don't think this will happen that quickly—quicker than that, but not very quickly.

Senator MURRAY. So you don't see the Clipper Chip becoming commonplace for 10 to 15 years?

Mr. KAMMER. Things happen faster now than they did 15 years ago, but I think it will be at least 5 years before any marketplace

choice emerges, Clipper or possibly something else. This is voluntary. People may pick something else.

Senator MURRAY. And you don't think that anybody can figure that out in the next 15 years?

Mr. KAMMER. DES still serves us well and it is 17 years old. DES' work factor, if you will, is 2 to the 56th. This is 2 to the 80th. It is 16 million times stronger than DES, Clipper is.

Senator MURRAY. Do you have any way of knowing if someone figures it out?

Mr. KAMMER. My guess is that it would be so rapidly disseminated on the Internet and people would be so proud of themselves that I would hear from many sources simultaneously.

Senator MURRAY. OK; thank you.

Senator LEAHY. Well, of course, on the Internet we found Pretty Good Program——

Mr. KAMMER. Protection, PGP.

Senator LEAHY. Pretty Good Protection. That zipped out there and now the government is raising issues about whether that was an unlawful exporting of encryption. We know how quickly things move. There is no reason to think that somebody else won't do that.

I am going to submit a number of questions for the record to both of you, if you don't mind. I have questions ranging everywhere from why one supplier of Clipper Chip and the obvious questions of monopoly that come out of that, to a number of other technical questions.

I appreciate your testimony, and I want to tell you that I am not an automatic fan of Clipper Chip or the proposals of the administration on this. I would ask you, if you go back over the questions and answers and you find there is more information and more material you want us to have, in all fairness, please feel free to bring it forth.

[The questions of committee members are found in the appendix:]

Ms. HARRIS. Thank you.

Senator LEAHY. Thank you. We will take about a 2-minute recess to set up for the next panel. Thank you very much.

[Recess.]

Senator LEAHY. We are back on the record.

Our first witness will be Whitfield Diffie, an engineer and cryptographer with Sun Microsystems, Inc. Mr. Diffie is the inventor of the concept of public key cryptography and one of the founding members of the International Association for Cryptographic Research.

Mr. Diffie, we will begin with you.

PANEL CONSISTING OF WHITFIELD DIFFIE, ENGINEER AND CRYPTOGRAPHER, SUN MICROSYSTEMS, INC., MOUNTAIN VIEW, CA, ON BEHALF OF THE DIGITAL PRIVACY AND SECURITY WORKING GROUP; AND STEPHEN T. WALKER, PRESIDENT, TRUSTED INFORMATION SYSTEMS, INC., GLENWOOD, MD

STATEMENT OF WHITFIELD DIFFIE

Mr. DIFFIE. Well, we know you hear about sculduggery in these things. My notes just disappeared.

Senator LEAHY. The dog ate them?

Mr. DIFFIE. I frankly don't know. I went back to pick up my notes and I can't find them.

Senator LEAHY. Would you like some more time?

Mr. DIFFIE. No, no; that is fine. Thank you. Maybe this will make up in freshness for what it lacks in preparation.

I want to thank you, to start with, for inviting me to this. This is sort of appropriate. You introduced me as the inventor of the concept of public key cryptography. I did it working with Marty Hellman at Stanford University nearly 20 years ago, and the concept we introduced that is, in fact, in the TSD 3600 over there in some sense created this whole problem because prior to that all cryptographically secure networks required a central administration that actually had the power to decrypt traffic. It had to hold keys in order to make introductions that would allow it to decrypt traffic, and the techniques that we had the privilege of pioneering have allowed systems like this in which the phones negotiate directly with each other and no third party is able to read the traffic. So I guess I deserve whatever happens.

Subsequently, I went to Northern Telecom. I say this just to emphasize that I have had some experience with communications security in the telecommunications environment. After a 12 years of that, I came to Sun Microsystems and I am now very involved with Internet and Internet sort of security and things of that kind.

I have three things I was asked to comment on, and let me try to get through them rather quickly. I view this from a broad perspective. I try not to get tied up in individual issues of this network of programs that are being proposed—the Clipper, the Capstone, the Digital Telephony bill, and the Digital Signature.

I believe there is a fundamental issue here of whether we should be using the power of technology to increase the privacy of citizens or to expand the power of the government, and I accept the legitimacy of that power in a lot of cases, to use electronic surveillance against its citizens and against other people.

I think there has been a lot of what I would call irresponsible comment to the effect that cryptography represents something new, it represents some sort of absolute privacy, and since this new thing has appeared, it needs to be regulated.

I think if you look back to the era of the Bill of Rights, you will see that at that time any two people could have a private conversation merely by having the common sense to walk 100 yards off away from people. They would know there were no tape recorders, no shotgun microphones, and they would be having a private conversation. Nobody in the world today has that assurance. If you are talking on a secure phone, if you are talking in a secure conference room, you are depending on the cooperation of hundreds of people who built and maintain those systems.

So individuals can no longer achieve privacy in the way they could then, and the impact of this—the credible impact, I believe, for our democracy is that the integrity of political speech, which frequently means the privacy of political speech, is something that is, in the Madisonian view, the root of the legitimacy of laws in a democracy.

I think that with the progress of technology, what has happened is that we are in a position where if we do not make it a national priority to protect individual privacy, to guarantee that when individuals want privacy they can have it, we will have an ebbing away of the privacy that is essential to the democratic process.

Now, since we are short of time here, let me turn quickly—it is a rare privilege to speak on an issue where it seems that matters of conscience and matters of business go side by side. Sun Microsystems does about half its business outside the country and we are proud to be part of what we regard as building the infrastructure of the future information society, and that infrastructure will, in particularly, be the infrastructure that will support the commerce of the future.

The infrastructure of commerce has always required security. Ships' holds, warehouses, bills of lading—all of this is the classical security machinery of commerce, and if we are going to have the promise that the information society offers, we are going to need to have international standards for security. They can't be something that are weighted to try to give particular advantages to particular governments, particular agencies, et cetera.

My final point—I was asked to comment on alternatives, and I see that light has turned yellow, which means I should be turning yellow, I suppose.

Senator LEAHY. No, no; don't worry about it. They give me some latitude around here, so go ahead. [Laughter.]

Mr. DIFFIE. I have been asked to speak on alternatives to this matter, and I think you can't speak about alternatives without asking first whether there is a problem and what the problem is, and therefore what the various possible solutions are.

In looking at the evidence that has been presented before this committee and other places for either the problems of law enforcement or intelligence, I don't find the evidence compelling. There is no question that particular sources of intelligence get closed off from time to time, but if you look at technical intelligence and particular technical law enforcement facilities, you will find they are growing by leaps and bounds.

In electronic surveillance, warrants—I haven't been able to get the exact percentage that are, so to speak, room bugs and the percentage that are taps, but I know that in many of these cases traditional bugging accounts for a good deal of the information, and bugs are getting smaller, higher fidelity, harder to detect, et cetera.

If you similarly look at intelligence, you find that electronic intelligence is expanding dramatically, and the reason is that improved particularly radio and mobile communication channels draw far more valuable traffic into vulnerable channels than ever is protected by the introduction of technical measures. I don't know if that will go on forever, but it has been progressing steadily for decades now.

On the other hand, one can say that, in fact, alternatives to this will come about of their own accord. If you look at cryptography as a security measure, you have no choice but to distinguish two cases, communications and storage.

Now, in communications the view is that the communications are ephemeral. You don't try to save your own cipher text. You don't

worry about having to get it back if the keys to a conversation are lost later. As a matter of fact, you particularly want them to go away. Senator Specter mentioned the various spy scandals and things, and worrying about keeping things secret. In fact, the two most dramatic spy scandals prior to Ames in our own recent history were both cryptographic spies who kept keying material after they were supposed to have destroyed it and then sold it to the KGB.

The advantage of a device like the original TSD 3600 or the STU–III is that it creates ephemeral keys that exist only for the duration of one conversation and then are destroyed when the conversation ends and cannot be rederived from any of the surviving information. On the other hand, to create escrow agents, no matter how carefully constructed, is to create keys that stay in existence for months or years or decades after the conversations that they protected, and that is to create a potential loophole of immense proportions.

On the other hand, if you look at cryptography to protect storage, then you have no choice at anything above the individual level but to provide alternative mechanisms of access to the information. If a corporation were to keep its records encrypted—and there would be many benefits to that; that would mean it could ship them out over the Internet to storage sites so that if its headquarters burned down it would be able to get them back immediately. It would nonetheless have to be sure that somebody other than one archivist or one controller or something like that had the keys that protected this information. There would have to be alternative mechanisms that would be under the control of the corporate officers and they would provide them——

Senator LEAHY. They go through some of those same questions about who has the keys even now in storing information in electronic files because you at least need a password to get into that file.

Mr. DIFFIE. Yes, although typically less things are being done cryptographically. Almost by definition, there are other ways other than passwords to get around them.

Senator LEAHY. It gives you a trap door.

Mr. DIFFIE. Well, we don't usually think of it that way. It is just sort of a normal maintenance matter that if you take the machine apart, then you get at the information in other ways.

Since I am aware of time, let me sum up by saying that suppose we make a mistake in this decision; then there are two ways we can make the mistake. We can either fail to adopt a key escrow system now and when one is perhaps necessary, or we can adopt a key escrow system when one is, in fact, not necessary. Which of those mistakes would be worse?

My own view is that if we fail to adopt one this year—this talk of getting out ahead of the curve, and so forth, is really not very much to the point. Given that the life cycle of electronic equipment is rather short—devices like that, people expect to replace every 2, 3, 5, or 7 years. If this market domination strategy for introducing new cryptographic equipment that has this back door built into it is taken up at any time—if it can succeed at all, it will succeed in a few years.

On the other hand, suppose we do adopt something, despite all its controls that I believe are very dangerous to the process of democracy and that represents a statement, in principle, somehow for the first time that people don't really have a right to have confidence in the measures they take to protect their own communications. Then I believe we will run the risk of building a bureaucracy that is now defending this new power that it has gotten, and that that would be very difficult to dislodge even if we subsequently decided it had been a bad idea.

Thank you very much.

[The prepared statement of Whitfield Diffie follows:]

PREPARED STATEMENT OF DR. WHITFIELD DIFFIE

I would like to begin by expressing my thanks to Senator Leahy, the other members of the committee, and the committee staff for the opportunity not only of appearing before this committee, but of appearing in such distinguished company.

I think it is also appropriate to say a few words about my experience in the field of communication security. I first began thinking about cryptography while working at Stanford University in the late summer of 1972. My feeling was that cryptography was vitally important for personal privacy and my goal was to make it better known. I am pleased to say that if I have succeeded in nothing else, I have achieved that goal. Today, cryptography is a bit better known. In 1978, I walked through the revolving door from academia to industry and for a dozen years was "Manager of Secure Systems Research" at Northern Telecom. In 1991, I took my present position with Sun Microsystems. This has allowed me an inside look at the problems of communication security from the viewpoints of both the telecommunications and computer industries. I am also testifying today on behalf of the Digital Privacy and Security Working Group, a group of more than 50 computer, communications and public interest organizations and associations dedicated to working on communications privacy issues.

THE KEY ESCROW PROGRAM

Just over a year ago, the Administration revealed plans for a program of key escrow technology best known by the name of its flagship product the Clipper chip. The program's objective is to promote the use of cryptographic equipment incorporating a special back door or trap door mechanism that will permit the Federal Government to decrypt communications without the knowledge or consent of the communicating parties when it considers this necessary for law enforcement or intelligence purposes. In effect, the privacy of these communications will be placed in escrow with the Federal Government.

The committee has asked me to address myself to this proposal and in particular to consider three issues:

- Problems with key escrow, particularly in the area of privacy.
- The impact of the key escrow proposal on American business both at home and abroad.
- Alternatives to key escrow.

ON SCOPE AND PERSPECTIVE

The problems of today are usually best viewed in historical perspective. A century ago, the world witnessed the development of the first global telecommunications systems, with the appearance of transoceanic cables and later radio. The new technology posed an unprecedented challenge to national sovereignty. Countries could still control the movement of people and goods across their borders, but ideas and information could now move around the world without being subject to the scrutiny of customs or immigration officials.

The challenge, of course, is one that the notion of national sovereignty and nation state survived. In part this is due to the rise of mechanisms of censorship and regulation to control the new media. In part it is due to the fact that telecommunications

[1] Dr. Diffie is also testifying on behalf of the Digital Privacy and Security Working Group, a group of more than 50 computer, communications and public interest organizations and associations working on communications privacy issues.

proved tremendously useful to governments themselves. The new tool was promptly exploited by the European colonial powers, particularly Britain, to bind their empires more tightly together than had ever been possible in the past.

Telecommunications transformed government, giving administrators real time access to their representatives in remote parts of the world. It transformed commerce, facilitating world wide enterprises and beginning the internationalization of business that has become the byword of the present decade. It transformed warfare by giving generals the ability to operate from the relative safety of rear areas and admirals the capacity to control fleets scattered across oceans.

Once again, we are in the midst of a revolution in telecommunications technology and once again we hear the warning that national security, and perhaps even national sovereignty, are in danger. As the most powerful country in the world and the country whose welfare is the most dependent on both the security of its own communications and its success in communications intelligence, the United States confronts this challenge most directly.

In the course of discussing the key escrow program over the past year, I have often encountered a piecemeal viewpoint that seeks to take each individual program at face value and treat it independently of the others. I believe, on the contrary, that it is appropriate to take a broad view of the issues. The problem confronting us is assessing the advisability and impact of key escrow on our society. This requires examining the effect of private, commercial, and possibly criminal use of cryptography and the advisability and effect of the use of communications intelligence techniques by law enforcement. In so doing, I will attempt to avoid getting bogged down in the distinctions between the Escrowed Encryption Standard (FIPS185) with its orientation toward telephone communications and the CAPSTONE/TESSERA/MOSAIC program with its orientation toward computer networks. I will treat these, together with the Proposed Digital Signature Standard and to a lesser extent the Digital Telephony Proposal, as a unified whole whose objective is to maintain and expand electronic interception for both law enforcement and national security purposes.

PRIVACY PROBLEMS OF KEY ESCROW

When the First Amendment became part of our constitution in 1791, speech took place in the streets, the market, the fields, the officè, the bar room, the bedroom, etc. It could be used to express intimacy, conduct business, or discuss politics and it must have been recognized that privacy was an indispensable component of the character of many of these conversations. It seems that the right—in the case of some expressions of intimacy even the obligation—of the participants to take measures to guarantee the privacy of their conversations can hardly have been in doubt, despite the fact that the right to speak privately could be abused in the service of crime.

Today, telephone conversations stand on an equal footing with the venues available then. In particular, a lot of political speech—from friends discussing how to vote to candidates planning strategy with their aids—occurs over the phone. And, of all the forms of speech protected by the first amendment, political speech is foremost. The legitimacy of the laws in a democracy grows out of the democratic process. Unless the people are free to discuss the issues—and privacy is an essential component of many of these discussions—that process cannot take place.

There has been a very important change in two hundred years, however. In the seventeen-nineties two ordinary people could achieve a high degree of security in conversation merely by the exercise of a little prudence and common sense. Giving the ordinary person comparable access to privacy in the normal actions of the world today requires the ready availability of complex technical equipment. It has been thoughtlessly said, in discussions of cryptographic policy, that cryptography brings the unprecedented promise of absolute privacy. In fact, it only goes a short way to make up for the loss of an assurance of privacy that can never be regained.

As is widely noted, there is a fundamental similarity between the power of the government to intercept communications and its ability to search premises. Recognizing this power, the fourth amendment places controls on the government's power of search and similar controls have been placed by law on the use of wiretaps. There is, however, no suggestion in the fourth amendment of a guarantee that the government will find what it seeks in a search. Just as people have been free to protect the things they considered private, by hiding them or storing them with friends, they have been free to protect their conversations from being overheard.

The ill ease that most people feel in contemplating police use of wiretaps is rooted in awareness of the abuses to which wiretapping can be put. Unlike a search, it is so unintrusive as to be invisible to its victim and this inherently undermines ac-

countability. Totalitarian regimes have given us abundant evidence that the use of wiretaps and even the fear of their use can stifle free speech. Nor is the political use of electronic surveillance a strictly foreign problem. We have precedent in contemporary American history for its use by the party in power in its attempts to stay in power?

The essence of the key escrow program is an attempt use the buying power and export control authority of government to promote standards that will deny ordinary people ready options for true protection of their conversations. In a world where more and more communication take place between people who frequently can not meet face to face, this is a dangerous course of action.

OTHER DIFFICULTIES OF THE PRESENT PROPOSAL

The objections raised so far apply to the principle of key escrow. Objections can also be raised to details of the present proposal. These deal with the secrecy of the algorithm, the impact on security of the escrow mechanism, and the way in which the proposal has been put into effect.

One objection that has been raised to the current key escrow proposal is that the cryptographic algorithm used in the Clipper Chip is secret and is not available for public scrutiny. One counter to this objection is that the users of cryptographic equipment are neither qualified to evaluate the quality of the algorithm nor, with rare exceptions, interested in attempting the task. In a fundamental way, these objections miss the point.

Within the national security establishment, responsibility for communication security is well understood. It rests with NSA. Outside of that establishment, particularly in industry, that responsibility is far more defuse. Individual users are not typically concerned with the functioning of pieces of equipment. They acquire trust through a complex social web comprising standards, corporate security officers, professional societies, etc. A classified standard foisted on the civilian sector will have only one element of this process, federal endorsement.

In explaining the rationale behind key escrow at the 1993 National Computer Security Conference, Clint Brooks of NSA, argued that key escrow was not a trap door, reserving that term for a more mathematical approach in which the algorithm is not kept secret. Brooks held that this idea had been rejected on the grounds that the trap door could be found and exploited by opponents. Ironically, a similar weakness lurks within the escrow approach, because the cost to an opponent of extracting the family key and unit key of a chip from the chips communications is only marginally greater than the cost of extracting the key for an individual message.

Finally, there are disturbing aspects to the development of the key escrow FIPS. Under the Computer Security Act of 1987, responsibility for security of civilian communications rests with the National Institute of Standards and Technology. Pursuant to this statute, the Escrowed Encryption Standard appeared as Federal Information Processing Standard 185, under the auspices of the Commerce Department. Apparently, however, authority over the secret technology underlying the standard and the documents embodying this technology, continues to reside with NSA. We thus have a curious arrangement in which a Department of Commerce standard seems to be under the effective control of a Department of Defense agency. This appears to violate at least the spirit of the Computer Security Act and strain beyond credibility its provisions for NIST's making use of NSA's expertise.

IMPACT ON BUSINESS

Business today is characterized by an unprecedented freedom and volume of travel by both people and goods. Ease of communication, both physical and electronic, has ushered in an era of international markets and multinational corporations. No country is large enough that its industries can concentrate on the domestic market to the exclusion of all others. When foreign sales rival or exceed domestic ones, the structure of the corporation follows suit with new divisions placed in proximity to markets, materials, or labor.

Security of electronic communication is as essential in this environment as security of transportation and storage have been to businesses throughout history. The communication system must ensure that orders for goods and services are genuine, guarantee that payments are credited to the proper accounts, and protect the privacy of business plans and personal information.

Two new factors are making security both more essential and more difficult to achieve. The first is the rise in importance of intellectual property. Since much of what is now bought and sold is information varying from computer programs to surveys of customer buying habits, information security has become an end in itself rather than just a means for ensuring the security of people and property. The sec-

ond is the rising demand for mobility in communications. Traveling corporate computer users sit down at workstations they have never seen before and expect the same environment that is on the desks in their offices. They carry cellular telephones and communicate constantly by radio. They haul out portable PCs and dial their home computers from locations around the globe. With each such action they expose their information to threats of eavesdropping and falsification barely known a decade ago.

Because this information economy is relentlessly global, no nation can successfully isolate itself from international competition. The communication systems we build will have to be interoperable with those of other nations. A standard based on a secret American technology and designed to give American intelligence access to the communications it protects seems an unlikely candidate for widespread acceptance. If we are to maintain our leading position in the information market places, we must give our full support to the development of open international security standards that protect the interests of all parties fairly.

POTENTIAL FOR EXCESSIVE REGULATION

The key escrow program also presents the spectre of increased regulation. FIPS185 states that "Approved implementations may be procured by authorized organizations for integration into security equipment." This raises the question of what organizations will be authorized and what requirements will be placed upon them? Is it likely that people prepared to require that surveillance be built into communication switches would shrink from requiring that equipment make pre-encryption difficult as a condition for getting "approved implementations"? Such requirements have been imposed as conditions of export approval for security equipment. Should industry's need to acquire tamper resistant parts force it to submit to such requirements, key escrow will usher in an era of unprecedented regulation of American development and manufacturing.

ALTERNATIVES TO KEY ESCROW

It is impossible to address the issue of alternatives to key escrow, without asking what, if any, is the problem.

In recent testimony before this committee, the FBI has portrayed communications interception as an indispensable tool of police work and argued that the utility of this tool is threatened by developments in modern communications. Unfortunately, this testimony uses the broader term "electronic surveillance" almost exclusively. Although it refers to a number of convictions, it names not a single defendant, court, or case. This raises two issues: the effectiveness of electronic surveillance in general and that of communications interception in particular.

It is easier to believe that the investigative and evidential utility of wiretaps is rising that to believe it is falling. This is partly because criminals, like everyone else, does more talking on the phone these days. It is partly because modern systems like provide much more information about a call, telling you where it came from in real time even when it is from a long way away.

With respect to other kinds of electronic surveillance, the picture looks even brighter. Miniaturization of electronics and improvements in digital signal processing are making bugs smaller, improving their fidelity, making them harder to detect, and making them more reliable. Forms of electronic surveillance for which no warrant is held to be necessarily, particularly TV cameras in public places, have become widespread. This creates a base of information that was, for example, used in two distinct ways in the Tylenol poisoning case of some years back.

Broadening the consideration of high tech crime fighting tools to include vehicle tracking, DNA fingerprinting, individual recognition by infrared tracing of the veins in the face, and database profiling, makes it seem unlikely that the failures of law enforcement are due to the inadequacy of its technical tools.

If we turn our attention to foreign intelligence, we see a similar picture. Communications intelligence today is enjoying a golden age. The steady migration of communications from older, less accessible, media, both physical and electronic, has been the dominant factor. The loss of information resulting from improvements in security has been consistently outweighed by the increased volume and quality of information available. As a result, the communications intelligence product has been improving for more than fifty years.

The situation, furthermore, is improving. The rising importance of telecommunications in the life of industrialized countries coupled with the rising importance of wireless communications, can be expected to give rise to an intelligence bonanza in the decades to come.

Mobile communication is one of the fastest growing areas of the telecommunications industry and the advantages of cellular phones, wireless local area networks, and direct satellite communication systems are such that they are often installed even in applications where mobility is not required. Satellite communications are in extensive use, particularly in equatorial regions and cellular telephone systems are being widely deployed in rural areas throughout the world in preference to undertaking the substantial expense of subscriber access wiring.

New technologies are also opening up new possibilities. Advances in emitter identification, network penetration techniques, and the implementation of cryptanalytic or crypto-diagnostic operations within intercept equipment are likely to provide more new sources of intelligence than are lost as a result of commercial use of cryptography.

It should also be noted that changing circumstances change appropriate behavior. Although intelligence continues to play a vital role in the post cold war world, the techniques that were appropriate against an opponent capable of destroying the United States within hours may not be appropriate against merely economic rivals.

If, however, that we accept that some measure of control over the deployment of cryptography is needed, we must distinguish two cases:

- The use of cryptography to protect communications and
- The use of cryptography to protect stored information.

It is good security practice in protecting communications to keep any keys that can be used to decipher the communications for as short a time as possible. Discoveries in cryptography in the past two decades have made it possible to have secure telephones in which the keys last only for the duration of the call and can never be recreated, thereafter. A key escrow proposal surrenders this advantage by creating a new set of escrowed keys that are stored indefinitely and can always be used to read earlier traffic.

With regard to protection of stored information, the situation is quite different. The keys for decrypting information in storage must be kept for the entire lifetime of the stored information; if they are lost, the information is useless. An individual might consider encrypting files and trusting the keys to memory, but no organization of any size could risk the bulk of its files in this fashion. Some form of key archiving, backup, or escrow is thus inherent in the use of cryptography for storage. Such procedures will guarantee that encrypted files on disks are accessible to subpoena in much the same way that file on paper are today.

In closing, I would like to as which would be the more serious mistake: adopting a key escrow system that we do not need or fail to move quickly enough to adopt one that we do.

It is generally accepted that rights are not absolute. If private access to high-grade encryption presented a clear and present danger to society, there would be little political opposition to controlling it. The reason there is so much disagreement is that there is so little evidence of a problem.

If allowing or even encouraging wide dissemination of high-grade cryptography proves to be a mistake, it is likely to be a correctable mistake. Generations of electronic equipment follow one another very quickly. If cryptography comes present such a problem that there is a popular consensus for regulating it, this will be just as possible in a decade as it is today. If on the other hand, we set the precedent of building government surveillance capabilities into our security equipment we risk entrenching a bureaucracy that will not easily surrender the power this gives.

NOTES:

I have treated some aspects of the subjects treated here at greater length in other testimony and comments and copies of these have been made available to the committee.

"The Impact of Regulating Cryptography on the Computer and Communications Industries" Testimony Before the House Subcommittee on Telecommunications and Finance, 9 June 1993.

"The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology" Testimony Before the House Subcommittee on Science and Technology, 11 May 1993.

Letter to the director of the Computer Systems Laboratory at the National Institute of Standards and Technology, commenting on the proposed Escrowed Encryption Standard, 27 September 1993.

Senator LEAHY. Thank you.

Mr. Walker, we had earlier the question asked of, the Justice Department whether you could use other encryption devices for voice communications through our computers. The answer was some-

what different than I had expected. I will turn it to you and let you do your own testimony.

STATEMENT OF STEPHEN T. WALKER

Mr. WALKER. Thank you very much, Mr. Chairman. My name is Steve Walker and I am the founder and President of Trusted Information Systems, an 11-year old computer security company. Before I started TIS, I had spent 22 years with the Defense Department at the National Security Agency, the Advanced Research Projects Agency, and the Office of the Secretary of Defense.

Before we get to the demo of an alternative to the answer that you got from the Justice Department, I would like to make a few comments and then move to the demo.

Senator LEAHY. Sure.

Mr. WALKER. I am opposed to the key escrow cryptography as proposed by the administration's Clipper initiative. I believe that any government program that is as potentially invasive of the privacy rights of American citizens as key escrow is should only be imposed after careful review by the Congress and the passage of legislation, legislation that is signed by the President and, if necessary, declared constitutional by the Supreme Court.

In 1968, we went through a very painful process of authorizing wiretaps under very stringent conditions, and I believe that the government imposition of key escrow procedures deserves no less careful consideration. I believe that many Americans will accept government-imposed key escrow if it is established through law and if the holder of the keys is in the judiciary branch of the government. But without such action, I suspect most Americans will remain firmly opposed to Clipper.

I am concerned that there appears to be very little business case for the administration's assertions that key escrow will maintain law enforcement's ability to wiretap criminals. I fear that, as presently being pursued, the Clipper initiative will be an expensive program that will yield few, if any, results.

I am actually angered that the government's fixation on law enforcement and national security interests has delayed the establishment of a digital signature standard for over 12 years and done considerable harm to the economic interests of the United States. Mr. Kammer talked about a digital signature standard and how important it was, but, in fact, because of the fixation on the interests of law enforcement and national security, we don't have one when we could have had it 12 years ago.

I am also opposed to continued imposition of export controls on products that employ cryptography that are already routinely available throughout the world, as we will discuss here in a moment. The only effects that these controls are having is to deny U.S. citizens and businesses protection of their own sensitive information from foreign and domestic industrial espionage, and to place U.S. information system producers at a severe disadvantage in a rapidly growing market. I also wish to say, and I am sorry Senator Murray is not here, that I very strongly support her bill, S. 1846, and Maria Cantwell's bill, H.R. 3627, in their attempts to alleviate this export control problem.

I was very pleased when Ray Kammer brought in the Clipper TSD and demonstrated it because I wanted to talk just for a minute about how we got into this mess, the Clipper mess, in some sense. This is the culprit that began it. This is a TSD that looks very much like the one that you used a few minutes ago, except at the end of the TSD 3600 there is a "D." This device was initially announced back in September 1992 by AT&T, with some publicity—two-page ads in Business Week and elsewhere—and it has DES in it. In some very real sense, it was the introduction of this device that caused NSA and the FBI to go into a flurry to try to find an alternative.

In January 1993, AT&T began shipping these devices. I got eight of them at that time, but they told us they were only on loan. You couldn't buy them, and they promised us there would be something better in April. This was in 1993. In April, when the administration announced the Clipper initiative, the same day AT&T pledged their support for it. Unfortunately, Clipper Chips were not ready and so AT&T cooled its heels.

Then very quietly, in August 1993, yet another device was introduced. This is the 3600 P. It has a proprietary algorithm in it, proprietary to AT&T. We don't know what its quality is relative to DES, but it can't be exported, so it must be pretty good.

These devices have been on sale—I bought this one from AT&T—since last August and they are now selling both the Clipper device that has an "E" after the 3600 for "escrow," presumably, and the P device to the marketplace. When you ask them what are their thoughts on this, they say, well, let's let the market decide what it wants. So part of the discussion this morning that you have already had about are people going to buy the 3600 escrow device—there already is an alternative that they can pick and let the market, in fact, decide.

In the interests of time, I have done a quick market analysis which I won't spend time on. I asked AT&T how many TSD's they expected to sell and I was told by one individual they expected to sell about as many as the STU–III's that are out there, the very popular classified phone systems. There are about 250,000 of those out there, and if you look at the chart comparing the number of wiretaps that are anticipated and the 500 million phones that are in the United States now, my estimate—and I basically challenge the administration to produce some contrary numbers that show I am wrong. If there are 250,000 such devices sold, there will be 2.5 key escrow calls intercepted each year. If the $16 million estimate for operating the key escrow centers is amortized across that, each one of those calls will cost $6.4 million.

Now, if the numbers are wrong, if we increase it by a factor of 10 or a factor of 100, when we get to the point where we have 25 million of these devices, 1 on every 20 telephones, we are still only going to get a key escrow call every 1½ days and it is still going to cost $64,000 for that call, which is twice the price of a current wiretap that doesn't involve cryptography.

I would like to switch for a moment to the export control situation just to emphasize the things that we have here on the side. The administration has asserted that export controls are not harmful to U.S. business because there are no commercially available

foreign products involving cryptography. Last year, the Software Publishers Association commissioned a study to look at this issue and we have our latest results over in this chart.

We have now found over 340 foreign products that involve cryptography coming from 22 countries around the world. One hundred fifty-five of these use DES and 70 of them at least use it with software. We have been able to purchase products from the companies listed on the bottom there and those are on display. The notebooks that we have there contain the product literature that we have on each of the products that are there. It is arguable that this is not an overwhelming number that we have found, but it certainly appears more significant than many people have suspected.

Another thing that we have found from our survey, though, that is frightening to me, at least, and to U.S. businesses is that those products that we obtained are DES software products. We got them from Australia, Denmark, Finland, Germany, Israel, Russia and the United Kingdom. We got them without any trouble at all. In many cases, these people have distributors around the world, sometimes in the United States. You can call a German company on an 800 number. Somebody in Connecticut answers it, and you will have a DES software product on your desk the next day. We cannot ship those back. We would be in complete violation of U.S. export laws.

The issue here is that it is not a level playing field. Our allies, our friends, in England and in Germany are routinely shipping products like this to us which we can't ship to them, and that is a very grave concern and why I have particular support for the——

Senator LEAHY. So if you were an American company with branches overseas and you wanted to use this, you would have the branches overseas buy the product from the source overseas and then ship to you the product that you would use back here?

Mr. WALKER. Well, if it was my company overseas, my subsidiary, I can get approval from the State Department. It takes about 6 months to do that, but you are right.

Senator LEAHY. Yes; I understand that. I am talking about a multinational.

Mr. WALKER. Multinational companies are routinely buying products from foreign sources. In my written testimony, I have several examples. A company called Semaphore in California listed about 15 examples of lost sales recently that they have encountered, and everyone has these experiences. Fortune Magazine this month has a two-page article in which the president of Sun and other companies talk about how serious this problem is and how little good it is doing anyone.

Senator LEAHY. The laptops that we are going to use in your demonstration didn't come with encryption capability already programmed in them, did they?

Mr. WALKER. No; they did not.

Senator LEAHY. Was it very difficult to add the DES program to it?

Mr. WALKER. No; the gentleman who did it is sitting behind me. It took him about a day to add it. Basically, if you wish, sir—yours looks like it is in working order there.

Senator LEAHY. The computer is in working order. That doesn't necessarily mean that I am going to know what I am doing with it.

Mr. WALKER. Well, it is going to be easy. I will explain it to you, sir.

Senator LEAHY. I have got the cursor on "talk" right now.

Mr. WALKER. Don't hit yet.

Senator LEAHY. I mean, it is so tempting. My hand is just twitching here.

Mr. WALKER. OK; go ahead. It is all right.

Senator LEAHY. No, no, I am not going to. Go ahead, go ahead.

Mr. WALKER. It is all right if you would like to do that.

These are basically Macintosh PowerBooks. They are actually last year's models. If we had had this year's models, it would run a little bit faster. This is a program that is available for about $70 from a company called Two Way Communications in San Diego, CA. It is routinely available to anybody who wants it. These laptops have built into them speakers and microphones, and therefore they have the ability to handle multimedia communications of all sorts.

Basically, what we did was obtain this piece of software from the San Diego Company which, incidentally, is written by a programmer in Moscow. That has nothing to do with the cryptography at all, just an indication of the worldwide nature of all of this. It has on it a button called "talk" which, if you hit the cursor, will allow you to talk to me. If you would like to do that, go ahead.

That is working.

Senator LEAHY. OK; now, it says "stop." Is that OK?

Mr. WALKER. Yes; when you are activating it, it will then give you the opportunity to turn it off by hitting the "stop" button. Now, if you notice down below there is a little button called "encrypt sound" just below the "talk" button. It is a little square.

Senator LEAHY. Yes.

Mr. WALKER. If you will just move the cursor down and press that, sir?

Senator LEAHY. Got it.

Mr. WALKER. Now, you are speaking to me in DES encrypted communications.

Senator LEAHY. All right.

Mr. WALKER. It doesn't sound any different than it did before.

Senator LEAHY. No. I am just going to adjust my volume here a little bit.

Mr. WALKER. The volume needs to be adjusted in the room.

Senator LEAHY. So, now, is the sound going through, encrypted at your end?

Mr. WALKER. Well, no. It is in the clear at my end.

Senator LEAHY. I mean, it is encrypted between here and where you are.

Mr. WALKER. Yes; if you would hit the "stop" button, then I will talk through you and be able to indicate to you how it would sound if you were intercepting this.

Senator LEAHY. I just hit the "stop" button.

Mr. WALKER. OK; now, I will turn mine on. The reason we do this one way right now—I mean, one at a time—is because of the

lack of power in these laptop computers. If we had PC's sitting here, then it would be much better.

Now, I am going to hit the "encrypt" button. Now, I am speaking to you encrypted. Can you hear me or do we need to adjust the——

Senator LEAHY. No; I can hear it.

Mr. WALKER. We are getting feedback through the speaker system, I am afraid. Now, if I decided I didn't want you to hear what I was doing anymore, I could hit the "encrypt" button again. This is what you would hear if you had the wrong key. I will turn it off so that we don't have to do that again. This is the same thing that they talked to us about with the tape that they were playing where you hear the white noise.

Essentially, all I did was change the key that I am using, and you didn't know what the key was and so what you heard was noise. So if you were somewhere out on the net intercepting this, that is what you would get if we didn't have the same key.

Basically, that is the demo. It is that laptop computers can be used as telephones or as communications vehicles over the Internet or anywhere else on a routine basis. This stuff is available right now, and adding cryptography to it was fairly trivial. It took a day or so to find where to put it in here and then just take DES from anywhere in the world and plug it in. The effect on you and me hearing this is, in fact, no different when it is encrypted than when it is not.

I will turn mine off. You can turn it back on if you would like.

Senator LEAHY. I hit "stop." I think I am off.

Mr. WALKER. I can hear you now.

Senator LEAHY. You can?

Mr. WALKER. Yes.

Senator LEAHY. Now, what do I do to turn this sucker off entirely?

Mr. WALKER. You just hit the "stop" button and close the top. The point of this is not that there is any magic here; in fact, that there isn't any magic here.

Senator LEAHY. But it also makes a point I asked earlier in the hearing of is it possible to just set this up with a commercial encryption program.

[Stephen T. Walker submitted the following materials:]

PREPARED STATEMENT OF STEPHEN T. WALKER

I am pleased to testify today about the concerns I share with many Americans about the Administration's Clipper Initiative and the negative impact that U.S. export control regulations on cryptography are having on U.S. national economic interests.

My name is Stephen T. Walker. I am the founder and President of Trusted Information Systems (TIS), Inc., an eleven year old firm with over 100 employees. With offices in Maryland, California, and England, TIS specializes in research, product development, and consulting in the fields of computer and communications security.

My background includes twenty-two years as an employee of the Department of Defense, the National Security Agency (NSA), the Advanced Research Projects Agency, and the Office of the Secretary of Defense. During my final three years in government, I was the Director of Information Systems for the Assistant Secretary of Defense for Communications, Command, Control, and Intelligence (C3I).

For the past three years, I have been a member of the Computer System Security and Privacy Advisory Board, chartered by Congress in the Computer Security Act of 1987 to advise the Executive and Legislative Branches on matters of national concern in computer security. In March 1992, the Board first called for a national re-

view of the balance between the interests of law enforcement/national security and those of the public regarding the use of cryptography in the United States. The Board has been heavily involved in this review, receiving public input on the Administration's Clipper initiative, announced by the President on April 16, 1993, and reaffirmed on February 4, 1994. I am also a member of the National Institute of Standards and Technology's (NIST) Software Escrowed Encryption Working Group, which is examining the possibilities for alternatives to the Clipper key escrow system.

OVERVIEW

My testimony today will include my concerns with the Administration's Clipper key escrow program and U.S. Government's rigid control of the export of products containing cryptography in the face of growing worldwide availability and easy export of such products by other countries. In Summary:

I am opposed to key escrow cryptography as proposed in the Administration's Clipper Initiative.

I believe that any government procedure that is as potentially invasive of the privacy rights of American citizens as key escrow should only be imposed after careful Congressional consideration and passage of legislation by the Congress, which is signed into law by the President and determined to be Constitutional by the Supreme Court. In 1968, properly authorized government wiretaps of private citizens were legalized through this process. Government imposition of key escrow procedures deserves no less careful consideration.

I believe that most Americans would accept government-imposed key escrow if it was established by law and if the key escrow center was located in the Judicial Branch of government.

I am concerned that there is not a sound "business" case to support the Administration's assertion that key escrow will maintain law enforcement's ability to wiretap the communications of criminals. I fear that as presently being pursued, the Clipper Initiative will be an expensive program that will yield few if any results.

I am angered that the government's fixation on law enforcement and national security interests has delayed establishment of a Digital Signature Standard (DSS) for over twelve years and done considerable harm to the economic interests of the United States.

I am also opposed to the continued imposition by the U.S. Government of export controls on products and technologies employing cryptography that are routinely available throughout the world. The only effects these controls have are to deny U.S. citizens and businesses protection for their sensitive information from foreign and domestic industrial espionage and to place U.S. information system products at a disadvantage in the rapidly growing international marketplace.

A PATTERN OF ADMINISTRATION INITIATIVES

A number of recent Administration initiatives have heightened the concerns of many Americans:

- The digital telephony initiative, in which the government wants to ensure that it can always tap everyone's phone when it has the legal authority to do so,
- The Clipper key escrow initiative, in which the Administration wants to be sure that it can easily break the cryptography of American citizens when it has the legal authority to do so,
- The Digital Signature Standard non-initiative, in which the government has repeatedly, for twelve years, failed to achieve a basic technological capability that is widely acknowledged as being essential to electronic commerce, and
- The continued imposition of controls on the export of cryptographic products in spite of clear evidence of foreign availability of similar products and foreign governments' failure to impose similar export controls, and in contrast to the massive relaxation of export controls in other areas of high technology.

All of these activities, taken together, lead one to the ominous conclusion that the Administration's goal is to severely restrict the average American's ability to protect his or her sensitive information with the hope that in so doing, it will also restrict such capabilities of criminals, terrorists, and those opposed to the United States.

All of these initiatives are symptoms of the fundamental national dilemma we face of finding a proper balance between:

- The rights of private individuals and organizations to protect their own sensitive information and, in effect, our national economic interests and
- The needs of law enforcement and national security interests to be able to monitor the communications of our adversaries.

Until we can strike a reasonable balance between these basic needs, this debate will continue. Unfortunately, the Administration's position is focused solely on the interests of law enforcement and national security to the exclusion of the rights of private citizens and the nation's economic interests.

I believe that only the Congress can determine where a reasonable balance lies between Americans' right to privacy and our national security interests.

We can no longer afford to have this determination being made exclusively by the Executive Branch.

CLIPPER KEY ESCROW

I would like to begin by summarizing my concerns with the Administration's key escrow initiatives.

Law enforcement and national security communications interceptions are vital functions of a modern government. I support these functions and encourage their continuation.

But the sky will not fall if we do not have Clipper key escrow or if cryptographic export controls are relaxed to levels consistent with worldwide availability. Law enforcement as we know it will not end if a few wiretaps encounter encrypted communications. And the nation's ability to listen in to the communications of its adversaries will not end if some of those intercepts encounter increased use of cryptography.

They had better not end, because both law enforcement wiretaps and national security intercepts are going to encounter ever-increasing amounts of encrypted communications no matter what the Administration does or does not do.

We must understand and accept the growing availability of cryptography worldwide as a basic fact of life. The ever-widening availability of cryptographic technology in the U.S. and overseas will make it harder day by day to monitor the communications of our adversaries, no matter what measures the Administration may attempt to take. There are no magic solutions to this issue, which originates in the very same technological advances that we are all taking advantage of in our daily lives.

We must also understand that those same technological advances are creating greatly improved techniques for exhaustively checking the key space of cryptographic algorithms such as DES and for factoring large prime numbers. A design for a system that could exhaustively check the key space of DES in 3½ hours was described at a public conference on cryptography last Summer. A group at Bellcore recently announced they had factored a 129 digit number, a new high.

The concept put forward by some in government that if we do not have key escrow or if we allow export of DES products, all our intelligence operations will suddenly fail, is false. On the contrary, key escrow will never be more than a small side show in the world of cryptography and DES cryptography will continue its rapid growth worldwide whether the US allows its export or not. Our government will be much better served by focusing on techniques to defeat known algorithms rather than promoting new techniques that are highly unpopular in the US and abroad.

TECHNOLOGY SHIFTS THREATEN THE WIRETAP BALANCE

Since 1968, when the wiretap provisions of the Omnibus Crime Control and Safe Streets Act went into effect, we seem as a nation to have found a constructive balance between the needs of law enforcement to intercept communications of suspected criminals and the desire of the public for the perception of privacy in its communications. The apparent successes that law enforcement has achieved through legally authorized wiretaps against organized crime, coupled with the difficulties cited by law enforcement officials in obtaining them, and the steady rate of 800 or so per year over the past decade all indicate that we probably have achieved about as good a balance on this issue as we can ever get.

But now technological advances threaten to upset this balance. The ready availability of good quality cryptography in inexpensive phone devices threatens to make it easy for those criminals who recognize that they may be tapped to protect themselves. The AT&T announcement in September 1992 of a relatively cheap Telephone Security device (TSD) that uses the Data Encryption Standard (DES) cryptographic algorithm to protect phone conversations apparently threw NSA and the FBI into high gear to find an alternative.

And bring on clipper

What emerged from this was the Clipper initiative, the goal of which is to give the American public very good cryptography that could, if necessary, be readily decrypted by authorized law enforcement officials. A firestorm of protests then followed from virtually all segments of the American public and many of our friends overseas that government-imposed key escrow is not something that they want.

In the midst of the flood of protests over violations of civil liberties and infringements of Bill of Rights that key escrow will cause and complaints about the use of a secret algorithm to protect unclassified information, several basic "laws" of the marketplace seem to have been overlooked. The Administration has never presented a "business plan" describing how Clipper will succeed in maintaining the ability of law enforcement to wiretap the phones of criminals. The lack of a fundamental understanding of how things work in a competitive marketplace shows up conspicuously throughout this story.

One of the first principles of business is to have your product ready for the market when the market is ready for it. In January 1993, following their September 1992 announcement, AT&T began shipping TSDs with DES. But pressure from the government apparently convinced AT&T to endorse the as yet unannounced Clipper program. So AT&T "loaned" the DES devices to their first customers with a promise that something "better" would be available in "April." And sure enough, on April 16, 1993, as the Administration announced Clipper, AT&T pledged its support.

Unfortunately, Clipper chips were not ready. So AT&T cooled its heels waiting for something to sell. Finally, in August 1993, AT&T quietly introduced another TSD that uses proprietary cryptographic algorithms, thus creating a major competitor for Clipper.

In effect, we have come full circle. In September 1992, the initial AT&T announcement was perceived by the government as a major threat to law enforcement. In August 1993, while waiting for Clipper chips, AT&T introduced a similar product that must represent a similar threat. AT&T is now selling both Clipper and non-Clipper TSDs in order to let the market decide which it wants.

What is the market for clipper?

In any business venture, it is important to understand the potential market for a product and to determine if one's market penetration will be sufficient to achieve one's goals.

For it to maintain law enforcement's ability to wiretap, the Clipper initiative must achieve a reasonably high market penetration. The problem is that very few people today will want to buy a telephone security device, even if it costs $50 instead of over $1,000. Very few residential users will bother, and those who do will find few people to talk to. Businesses will buy telephone security devices for their executives to protect strategic business communications, but the vast bulk of routine business communications will go unprotected.

Today there are estimated to be over 500 million phones in residential and business use in the U.S. When asked how many TSDs AT&T expected to sell, one estimate was at least as many as the popular STU–III secure phones for use with classified information. There are approximately 250,000 STU–IIIs installed today.

Numbers like these represent a very reasonable business case for AT&T, but will they allow the Clipper program to achieve its goal of solving the law enforcement wiretap problem?

If the above estimates are correct, in a few years roughly five one-hundredths of one percent (0.05%) of America's phones will be protected by TSDs (250,000/500,000,000). Of course many of these will use the proprietary algorithm rather than Clipper. But we will optimistically assume that this percentage represents the situation with Clipper TSDs in five years.

Now if one analyzes the average number of court-authorized wiretaps over the past fifteen years, one can reasonably conclude that 1,000 such wiretaps per year would be a reasonable projection for the near future. One could further assume that each court-ordered wiretap results in as many as five actual phone taps. This leads to an estimate of 5,000 physical wiretaps per year. A typical cost for a wiretap operation not involving cryptography has been estimated at $50,000 to $60,000.

In the Administration's proposed key escrow plan, there will be two key escrow centers, one at NIST and one at Treasury, that, when fully operational, will be available 24 hours a day, seven days a week, year round. These will each require a staff of at least ten people at a labor cost of $ 1.5M per year. The non-labor costs of each center will be another $ 1.5M leading to a total annual cost for both centers of $6.0M.

No estimate exists for how much it has cost to develop and promote the Clipper initiative. In a business analysis, it would be important to amortize these costs over

the expected value of the "product," but for now all we have to use is the estimated cost of operating the centers.

If Clipper TSDs represent 0.05% of the phones in America and there are 5,000 taps per year, then law enforcement officials can reasonably expect to encounter on average 2.5 Clipper key-escrowed phone taps per year, or one every 145 days. If the cost of the key escrow center operations is amortized over 2.5 calls per year, each key-escrowed wiretap will cost $2.45M ($50 K for wiretap and 2.4M for escrow center expenses). At $1,000 per TSD, 250,000 will cost the consumer $250M.

But suppose the STU–III equivalent estimate is far too conservative for sales of TSDs. If sales are 2.5 million devices (0.5% of all phones), this will lead to interception of approximately 25 key-escrowed phone calls per year, about one every fifteen days. If the key escrow centers' costs are amortized over 25 calls per year, each key-escrowed wiretap will cost $290,000 ($50 K for wiretap and $240K for escrow center expenses). If TSD prices fall in an expanded market to $500 per TSD, 2.5M devices will cost the consumer $1.25B.

If the demand for TSDs is truly enormous, reaching 5% of all phones in the U.S., one could expect about one key-escrowed wiretap every day and a half. In this case, the cost of a key-escrowed wiretap will rise to $74,000 ($50 K for wiretap and $24,000 for escrow center expenses). Only in this last case does any form of cost benefit tradeoff for the cost of a wiretap make sense. Even if prices were to fall to $100 per TSD, 25M will cost the consumer $2.5B.

Number of Clipper Telephone Security Devices:	250,000	2,500,000	25,000,000
Percent of U.S. phones:	00.05%	00.5%	5%
Number of Key Escrow taps/yr:	2.5	25	250
One call to key escrow center every:	145 days	15 days	1.5 days
Cost per escrowed key call:	$2.4M	$240,000	$24,000

This scenario assumes that the population of phones likely to be tapped is roughly the same as that of the general population. Unfortunately, this is unlikely to be true since, on one hand, the average criminal who doesn't realize he is likely to be tapped is unlikely to bother with any form of TSDs and so can be wiretapped using conventional means and, on the other hand, the "sophisticated" criminal, who understands what he may be up against, will almost certainly buy non-key escrowed TSDs. Under these circumstances, 2.5 key-escrowed calls per year is probably very optimistic.

Now there are those who say, If only one of those calls is a World Trade Center bomb plot, it will all be worth it!" But the World Trade Center bombers went back for a deposit on the rental truck they blew up. If they are the types we are up against, they will not have enough sense to use a TSD. And as pointed out above, the sophisticated criminal will surely know enough to not buy a key-escrowed TSD.

A contradictory story has also been put forth that claims that the Administration never intended to catch criminals using key escrow. In this version, the intent was to introduce cryptographic capabilities that are substantially better than what is available now and to include key escrow to deny their use to criminals. If this is the "real" reason for Clipper, then the Administration must understand that they will never get any wiretap calls for key escrow. If so, one must anticipate that the extensive protections now being planned for the escrowed keys will diminish over time from disuse. If this happens, all those who bought the "stronger" encryption capability will then become vulnerable to trivial decryption.

The Administration has stated that its plan is to buy enough TSDs to flood the market, thus making them so cheap that everyone will buy them. Their plan for "flooding" the market is to buy 9,000 devices using funds confiscated from criminals. Such a purchase will have little effect either in achieving the installed base necessary for key escrow to work properly or in reducing the price to a level where the devices are pervasive.

Even if every factor in this analysis is slanted in favor of Clipper, it is difficult to see how this program is going to help law enforcement maintain its ability to wiretap criminals. Clipper is an expensive program for both the government and the consumer that shows little if any promise of achieving its goal.

International aspects of key escrow

The Administration has stated that Clipper systems with key escrow will be exportable. The question remaining to be answered is will anyone outside the U.S. be interested. In July 1992, NSA agreed that certain encryption algorithms that were limited to 40-bit key lengths could be exportable. But 40-bit key lengths are so weak that no one inside or outside the U.S. would want them. It is clear that foreign governments may want key escrow systems to allow them to monitor communications, but their citizens will generally share the concerns of most Americans.

It may be possible for governments to work out bilateral agreements to share escrowed keys (though little progress has been reported to date), but this will do nothing for the growing need of multinational companies to communicate with others across international boundaries. The international aspects of key escrow remain a thorny problem, which will defy solution for a long time.

The capstone tessera program

Apparently when AT&T announced its DES TSD in late 1992, NSA had already been working on a program called Capstone which was to provide good quality cryptography and key escrow for computer communications. Applying these techniques to telephones required only a stripped down Capstone, which came to be called Clipper.

Capstone is a key ingredient in a program to provide information security for the Defense Message System and other programs within the Department of Defense. It is also being pushed for a wide variety of other programs within the government including the IRS, Social Security, and even Congressional systems.

Providing good cryptographic protection in a computer communications environment is much more difficult than in a telephone context. The ease with which a user can manipulate his or her text either before passing it to the Capstone process or after it has been encrypted makes it very difficult to ensure the effectiveness of the result. Also, the technologies involved in the present implementations of the Skipjack algorithm, while sufficient for telephone and low speed computer communications, will not easily scale to meet the needs of high speed computer communications.

Because it uses a secret algorithm, Capstone and the products that use it will only be available in hardware implementations such as the NSA Tessera PCMCIA card. It has been suggested that if the interfaces that Tessera uses could be generalized so that other cryptographic algorithms could be implemented in compatible packages, the Tessera program could have a much greater market penetration.

The Government has stated that Tessera will be exportable. If such common cryptographic interfaces existed, mass market software vendors who support Tessera could integrate cryptographic functions into their applications without concern for export controls on their products and vendors within individual countries could build Tessera equivalent PCMCIA cards using alternative cryptographic algorithms. Such a development would provide a fundamental increase in the market for cryptographic products and thus increase the chances for market penetration of products such as Tessera. At this time, it is unclear whether NSA will choose to generalize the Tessera interfaces to allow cards with other algorithms to coexist.

Strengths of clipper

I am convinced that Skipjack, the cryptographic algorithm in Clipper, is a very good algorithm. I also believe that procedures can be developed for protecting escrowed keys that will provide reasonable assurance that the keys will not be compromised under normal circumstances. I have known many of the people at NIST and NSA who have worked on this program for many years. I believe they are honest, well-intentioned people who are doing the best job they can to protect the interests of the law enforcement and national security communities.

My concerns are not with the strengths of this program or the integrity of the people who have put it together but with whether there is any practical chance that it will achieve its goals and whether the American people are ready for key escrow.

What should Congress do?

For any form of key escrow system to work, it must have the confidence of the American people. The Administration claims that it does not need legislation to impose key escrow, that it is operating entirely within the provisions of the wiretap statutes. This may be legally correct, but we should take lessons from the past on how to convince people to accept ideas that do not immediately seem to be in their best interests.

At least once before in modern times, the government was faced with convincing the American public to allow something that did not seem in the best interests of

the average citizen, that is, to allow the government to wiretap phones. But in 1968, Congress passed and the President signed a law that established a balance on the wiretap issue that appears reasonable to most of us.

If key escrow is the vital answer to encrypted wiretaps as the Administration claims, we should follow the same process we did for authorizing wiretaps:

(1) Congressional debate,

(2) Passage of legislation,

(3) Presidential signature, and

(4) Judicial review.

This full process is necessary before the American people will accept key escrow. The only excuse for not doing this seems to be that the process will take too long. But the reaction to date indicates that by not taking the time for the legislative process, the Clipper program will be little more than a program the government imposes on itself.

I strongly recommend that the Administration propose legislation that would give key escrow the same legal standing as court-ordered wiretaps. If the Administration does not take this action soon, I believe the Congress should act on its own to review this concept and determine if key-escrowed communications should be imposed on the American people.

THE DIGITAL SIGNATURE NON-INITIATIVE

Key escrow is not the only instance in which the Administration has focused almost exclusively on the law enforcement and national security side of an important issue. In almost total contrast to the haste with which the Clipper initiative has proceeded, the government's efforts over the past decade to establish a digital signature standard, an essential tool in any form of electronic commerce, have failed miserably. The background of this incredible failure should be very embarrassing to someone, but it appears there are so many participants that no one needs to take the blame.

According to a recent GAO report, this odyssey began in the early 1980s when the National Bureau of Standards (NBS, now NIST) sought a public key encryption standard to complement the DES. No progress was made even though nearly everyone acknowledged the essential need for such a capability and that the technology necessary for it already existed in the RSA public key encryption algorithm among others.

In the 1988 hearings on the progress of the Computer Security Act, the Directors of NSA and NBS were pressured to get on with establishing a public key encryption standard. In the recently released, highly censored proceedings of the joint NSA–NBS Technical Working Group, the tortuous deliberations toward a DSS are evident. Despite the ready availability of technology such as RSA, which could have provided a DSS as early as 1982, the government persisted in seeking an alternative with limited capabilities.

In the House Subcommittee on Science hearing on Internet Security, March 22, 1994, Mr. Lynn McNulty, Associate Director of the NIST National Computer Systems Laboratory, testified that:

> * * * our strategy * * * was to develop encryption technologies that did not do damage to the national security or law enforcement capabilities of this country. And our objective in developing the digital signature standard was to come out with a technology that did signatures and nothing else very well. It could not be used for either encryption or to provide key management or key distribution techniques for other symmetric encryption technologies.

With these constraints, the government placed itself in a very difficult situation that it has proceeded to make very much worse with time.

In August 1991, after considering at least four alternatives, NIST finally announced with much fanfare the selection of the Digital Signature Algorithm (DSA) for the DSS. NIST stated that this algorithm, patented by an NSA employee, would be royalty-free to all parties, an attractive offer since the use of RSA or other public key alternatives would require royalty payments to RSA Data Security, Inc., or Public Key Partners (PKP). A royalty-free signature algorithm was sufficiently attractive that many felt DSA could succeed against the already popular RSA algorithm.

The initial public comment period on the DSS selection brought mostly technical comments on the algorithm itself. Following this there was a long silent period during which NIST's only comment was that the lawyers were working on patent is-

sues. It seems there was a German, Professor Doctor C.P. Schnorr, who had a U.S. patent that he claimed was infringed upon by the DSA. NIST visited Professor Doctor Schnorr seeking to work out the patent issues. Apparently PKP did also, because in early 1993, PKP told the government that they now had the rights to Professor Doctor Schnorr's patent and that use of DSA by the government would infringe upon their patent rights.

In order to resolve this problem, NIST announced in June 1993 that they intended to give PKP an exclusive license to the DSA. The U.S. Government would have free use of DSA, but everyone else, including foreign governments, would have to pay royalties to PKP. This situation was very different from the August 1991 proposal. Now the only advantage of DSA over its well-established rival RSA was gone. The government wanted DSA because it could not be easily used for functions other than digital signature. But the public and other governments could no longer perceive any advantage to DSA.

The public comments, including several from foreign governments, on this NIST licensing proposal were overwhelmingly negative. Again the government's lack of any sense of the impact of this on the marketplace was apparent. Another long period of silence by the government extended from late summer 1993 until early 1994.

Then on February 4, 1994, as part of the Clipper approval announcement, NIST stated that the exclusive licensing of DSA to PKP would not take place, and it was the government's intention that the DSA would be available to anyone free of royalties. When asked what the government would do now to make this possible, the response was they would either (1) continue trying to negotiate a deal with PKP, (2) take the process to courts to prove that DSA did not infringe upon PKP's patents, or (3) develop a new algorithm. There was, of course, no timetable for resolving these alternatives.

So now we are no better off than we were in mid-1991 or perhaps even 1982. But today there are major commercial activities that are using RSA as the basis for digital signatures and there are major government programs, such as the IRS modernization effort, that must have a digital signature capability to succeed. NISTs present advice to government programs in need of a digital signature capability is to do whatever they want.

Recalling Mr. McNulty's testimony from above, we have another example of the government's insistence that law enforcement and national security interests totally dominate those of the public and civilian government. The result is that a capability that could have been available as a government standard in 1982 and is now a defacto commercial world standard has been held back for twelve years, and there remains no real prospect for when this issue will be resolved.

What should Congress do?

Unfortunately, in this case it is difficult to suggest what the Congress can do.

It would be unusual but not out of the realm of possibilities for the Congress to mandate the use of an existing industry standard for digital signatures for all government programs involving electronic commerce. The clear failure of the Executive Branch to find a suitable alternative after twelve years of searching and the urgent needs of government and commercial interests to have a readily available means for signing electronic documents would justify such a step by the Congress.

EXPORT CONTROL OF CRYPTOGRAPHY

And there are other examples of how the government's dominant concern for national security and law enforcement capabilities has driven the U.S. down paths that harm our national economic interests.

Since the publication of the DES as a U.S. Federal Information Processing Standard (FIPS) in 1977, cryptography has shifted from the exclusive domain of governments to that of individuals and businesses. DES in both hardware and software implementations is a defacto international standard against which all other cryptographic algorithms are measured.

The controversy that arose as soon as DES was published concerning whether it had weaknesses that intelligence organizations could exploit fostered the highly fruitful academic research into public key cryptography in the late 1970s. Public key algorithms have the major advantage that the sender does not need to have established a previous secret key with the recipient for communications to begin. Public key algorithms, such as RSA, have become as popular and widely used as DES throughout the world for integrity, confidentiality, and key management.

Software publishers association study

The Administration has asserted that export controls are not harming U.S. economic interests because there are no foreign cryptographic products and programs

commercially available. Implementations of DES, RSA, and newer algorithms, such as the International Data Encryption Algorithm (IDEA), are available routinely on the Internet from sites all over the world. But according to the Administration, these do not count as commercial products.

In order to understand just how widespread cryptography is in the world, in May of 1993, the Software Publishers Association (SPA) commissioned a study of products employing crpytography within and outside the U.S. There was a significant amount of knowledge about specific products here and there, but no one had ever tried to assemble a comprehensive database with, where possible, verification of product availability. I reported the results of this survey in hearings before the Subcommittee on Economic Policy, Trade and Environment, Committee on Foreign Affairs, U.S. House of Representatives last October.

Information on new products continues to flow in daily. As of today:

- We have identified 340 foreign hardware, software, and combination products for text, file, and data encryption from 22 foreign countries: Argentina, Australia, Belgium, Canada, Denmark, Finland, France, Germany, Hong Kong, India, Ireland, Israel, Japan, the Netherlands, New Zealand, Norway, Russia, South Africa, Spain, Sweden, Switzerland, and the United Kingdom.
- Of these, 155 employ DES either in hardware of software.
- We have confirmed the availability of 70 foreign encryption software programs and kits that employ the DES algorithm. These are published by companies in Australia, Belgium, Canada, Denmark, Finland, Germany, Israel, the Netherlands, Russia, Sweden, Switzerland, and the United Kingdom.
- Some of these companies have distributors throughout the world, including in the U.S. One German company has distributors in 14 countries. One U.K. company has distributors in at least 13 countries.
- The programs for these DES software products are installed by the users inserting a floppy diskette; the kits enable encryption capabilities to be easily programmed into a variety of applications.

A complete listing of all confirmed products in the database is identified in Attachment 1.

As part of this survey, we have ordered and taken delivery on products containing DES software from the following countries: Australia, Denmark, Finland, Germany, Israel, Russia, and the United Kingdom.

Foreign customers increasingly recognize and are responding to the need to provide software-only encryption solutions. Although the foreign encryption market is still heavily weighted towards encryption hardware and hardware/software combinations, the market trend is towards software for reasons of cost, convenience, and space.

- On the domestic front, we have identified 423 products, of which 245 employ DES. Thus, at least 245 products are unable to be exported, except in very limited circumstances, to compete with the many available foreign products.
- In total, we have identified to date 763 cryptographic products, developed or distributed by a total of 366 companies (211 foreign, 155 domestic) in at least 33 countries.

DES is also widely available on the Internet, and the recently popularized Pretty Good Privacy encryption software program, which implements the IDEA encryption algorithm, also is widely available throughout the world.

The ineffectiveness of export controls is also evident in their inability to stop the spread of technology through piracy. The software industry has a multibillion dollar worldwide problem with software piracy. Mass market software is easy to duplicate and easy to ship via modem, suitcase, laptop, etc. Accordingly, domestic software products with encryption are easily available for export—through illegal but pervasive software piracy—to anyone who desires them.

Foreign customers who need data security now turn to foreign rather than U.S. sources to fulfill that need. As a result, the U.S. Government is succeeding only in crippling a vital American industry's exporting ability.

Frequently heard arguments

There are a series of arguments frequently heard to justify continued export control of cryptographic products.

The first argument is that such products are not available outside the U.S., so U.S. software and hardware developers are not hurt by export controls.

The statistics from the SPA survey prove that this argument is false!

A second argument is that even if products are available, they cannot be purchased worldwide.

Our experience with purchasing products indicates that this also is not true. We have found 462 companies in 33 foreign countries and the U.S. that are manufacturing, marketing, and/or distributing cryptographic products, most on a worldwide basis. The names of these companies are listed in Attachment 2.

All the products we ordered were shipped to us in the U.S. within a few days. The German products were sent to us directly from their U.S. distributors in Virginia and Connecticut, respectively. Our experience has been that if there is paperwork required by the governments in which these companies operate to approve cryptographic exports, it is minimal and results in essentially immediate approval for shipping to friendly countries.

A third argument frequently heard is that the products sold in other parts of the world are inferior to those available in the U.S.

We have purchased products from several sources throughout the world. We ordered DES-based PC file encryption programs for shipment using routine channels from:

- Algorithmic Research Limited (ARL), Israel
- Sophos Ltd., UK
- Cryptomathic A/S, Denmark
- CEInfosys GmbH, Germany
- uti-maco, Germany
- Elias Ltd., Russia (distributed through EngRus Software International, UK)

The products we obtained from these manufacturers and distributors were in every case first-rate implementations of DES. To better understand if foreign products are somehow inferior, we have examined several of these products to see if we can detect flaws or inherent weaknesses.

What we have found in our limited examination is that while these products generally use fully compliant DES implementations, they sometimes do not make use of all the facilities that might be available to them. The result is a full-strength DES product that is fully adequate for protecting commercial sensitive information but would not meet the strict requirements of a full national security product review.

Two examples of facilities that these products do not fully utilize are:

- Initialization Vector (IV) (data added to the beginning of text to be encrypted to ensure synchronization with the decryption process). Frequently, these simple file encryption products use the same IV everytime. A product designed for protecting national security information would vary the IV each time.
- Key Generation: Frequently, these products use an encryption key derived from a string of text that is typed in by the user. Users may tend to use the same simple alphanumeric text strings to encrypt multiple files. A product designed for protecting national security information would generate a truly random encryption key, usually with each use.

It is important to note that there appears to be no difference between foreign and U.S. commercial products in the use of these simplifications.

A fourth frequently heard argument is that many countries have import restrictions that would prevent U.S. exports even if the U.S. relaxed its export controls.

While our surveys has focused on the ease of importing products into the U.S., we have noted that many of the companies in our survey have distributors throughout the world. There may be countries that restrict imports of cryptography just as there may be those that restrict internal use of cryptography. But we are unaware of any countries in this category.

Other countries have relaxed export controls

Our survey results also point to a much more ominous finding! Apparently the controls imposed by the U.S. Government on export of cryptographic products from the U.S. are far more restrictive than those imposed by most other countries, including our major allies. The effect of this most unfortunate situation is to cripple U.S. industry while our friends overseas appear to be free to export as they wish.

The U.S. imposes very strict rules on the export of cryptographic products. In general, applications for the export of products that use DES will be denied even to friendly countries unless they are for financial uses or for U.S. subsidiaries. We have been told repeatedly by the U.S. Government that other countries such as the United Kingdom and Germany have the same export restrictions that the U.S. does.

But our experiences with the actual purchases of cryptographic products show a very different picture.

We know that companies in Australia, Denmark, Germany, Israel, South Africa, Sweden, Switzerland, and the United Kingdom are freely shipping DES products to the U.S. and presumably elsewhere in the world with no more then a few days of government export control delay, if any. Sometimes the claim is that they have to "fill out some papers," but it's no big problem. In Australia, we are told, the exporting company must get a certificate that the destination country does not repress its citizens. Many countries allow shipment so long as it is not to former CoCom restricted countries (the former Soviet block and countries that support terrorism).

Our experience with these purchases has demonstrated conclusively that U.S. business is at a severe disadvantage in attempting to sell products to the world market. If our competitors overseas can routinely ship to most places in the world within days and we must go though time-consuming and onerous procedures with the most likely outcome being denial of the export request, we might as well not even try. And that is exactly what many U.S. companies have decided.

And please be certain to understand that we are not talking about a few isolated products involving encryption. More and more we are talking about major information processing applications like word processors, databases, electronic mail packages, and integrated software systems that must use cryptography to provide even the most basic level of security being demanded by multinational companies.

Demonstrations of available cryptographic products

We have before us today several examples of cryptographic products that were lawfully obtained in the United States from foreign vendors:

- AR DISKrete: produced by Algorithmic Research Limited (ARL), Israel. Uses DES disk/file encryption to provide PC security and access control.
- EDS: produced by Sophos Ltd., UK. DES-based PC file encryption package.
- F2F (File-to-File): produced by Cryptomathic A/S, Denmark. DES-based PC file encryption utility.
- Softcrypt: produced by CElnfosys GmbH, Germany. DES-based PC file encryption utility.
- SAFE–GUARD Easy: produced by uti-maco, Germany. DES-based PC file encryption utility.
- EXCELLENCE for DOS: produced by Elias Ltd., Russia; distributed through EngRus Software International, UK. GOST-based (Russian DES equivalent) PC file encryption utility.

In addition to these products, we have the complete set of notebooks of product literature we have gathered to confirm the information in our worldwide survey of cryptographic products.

We also have a demonstration of the power of the digital revolution and the impact it will have on all our communications in the future. Traditionally, when we think of voice communications, we think of the telephone in its many forms (desk, cordless, cellular, car). However, many modem computer workstations now have the ability to carry voice as well as other multimedia communications. Routinely today on the Internet, voice conferences are held over packet switched communications networks.

Today we have a demonstration using two off-the-shelf Apple Macintosh PowerBooks that come with both speakers and microphones that enable software programs such as Talker from 2 Way Computing, Inc., of San Diego, CA, to transform a laptop computer into a telephone.

With this laptop computer telephone, it is easy to protect phone conversations from eavesdroppers. Since all the telephone functions are performed in software, it is trivial to add an encryption algorithm, such as the DES, to the software and provide good quality encryption to the digitized speech.

Export control of information in the public domain

The U.S. International Trade in Arms Regulations (ITAR) govern what products can and cannot be subjected to export controls. These regulations clearly define a set of conditions in which information considered to be in the "public domain" can not be subject to controls. In the ITAR itself; public domain is defined as information that is published and that is generally accessible or available to the public:

- Through sales at bookstores,
- At libraries,
- Through patents available at the patent office, and

- Through public release in any form after approval by the cognizant U.S. Government department or agency.

The Data Encryption Standard has been openly published as a Federal Information Processing Standard by the U.S. Government since 1977. Implementations of it in hardware and software are routinely available in the U.S. and throughout the world. Publication of software programs containing DES in paper form are permitted because of the First Amendment in the Bill of Rights. But the export of DES as hardware or software remains subject to export control despite its clearly being in the public domain.

One frustrating and somewhat humorous result of this situation occurred recently when NIST published a FIPS that contained source code for DES. In paper form, the Automated Password Generation Standard, FIPS 181, is acceptable for worldwide dissemination. But when NIST made the FIPS available over the Internet without an export restriction notice, it was immediately copied by computers in Denmark, the UK, and Taiwan. When it was pointed out that NIST's actions were in apparent violation of the ITARs, they quickly moved the file to a new directory with an appropriate export prohibition notice. Now FIPS 181 is available from hosts throughout the world along with the notice that export from the U.S. is in violation of U.S. export control laws.

NIST "exported" source code for DES with apparent immunity. Phil Zimmerman is still being investigated by the U.S. government and facing a four year imprisonment for alledgedly doing nothing more.

Unfortunately, U.S. companies are not allowed to treat the export of DES in quite so simple a manner. As discussed earlier, DES is routinely available anywhere in the world. It meets the definition of "in the public domain" on numerous levels. And yet U.S. companies are prevented from exporting it other than to Canada. This situation is yet another example of the inconsistencies of U.S. export control policies.

Industrywide experiences

Some companies do try to compete and offer excellent DES-based products in the U.S. But because of the export restrictions, they must develop weaker versions for export if they wish to pursue foreign markets. Many companies forgo the business rather than spend extra money to develop another inferior product that cannot compete with products widely available in the market.

The government already has a measure of lost sales and dissatisfied customers in the number of State Department/NSA export license applications denied, modified, or withdrawn. However, it is impossible to estimate accurately the full extent of lost sales. Many potential customers know that U.S. companies cannot meet their demand and thus no longer require. Conversely, most major companies have given up even trying to get export approvals for DES to meet customer demand.

One U.S. company, Semaphore Communications Corporation, that makes products using DES encryption has provided the following comments on their recent experiences (quoted from a letter dated 4/20/94 to Stephen T. Walker from William Ferguson of Semaphore):

> As a small company with limited resources, we have chosen to get an assessment directly from the NSA prior to investing too many resources in pursuing the situations, as the NSA Export Office is the ultimate authority on whether any export license will be granted; or the U.S. companies with familiarity of the export regulations have advised us of their position before we invested too many resources.

The recent short-list of opportunities include:

1. NATO: order placed by SHAPE Technical Centre in 11/93 as precursor of NATO-wide security plan; pre-order query to State Dept. gave verbal approval as shipment was to an APO address: on submitting license application, NSA denied permission to ship. NATO officials are currently trying to get permission from NSA, but have thus far been denied.
2. Hong Kong Immigration Department: project to secure network communications for all department sites with fully redundant scheme: sought ruling before bidding in partnership with AT&T; denied 4/93. All competitors bid Racal; as a British company they had no restrictions.
3. Norway Telecom: planning secure network for government and financial users using single solution: sought ruling before bidding; told use sounded too general and export office would have difficulty approving. 10/93.
4. Dutch National Police computer network: application to secure entire national data network: advised would not be granted permission when seeking pre-bid rul-

ing, 11/93. Attempted to have our application viewed in same context as open license granted to DEC and IBM for similar equipment, but advised would need letters from all Dutch government agency department heads for any consideration. This effort would have required more than three months of effort by company executive located in Holland. Deemed too expensive for only one project.

5. Michelin: seeking solution to secure global network including all US-based, ex-Firestone facilities: when advised of export restrictions, Michelin rejected US-based technology to seek other solution; 4/93.

6. Volkswagen: in planning of security strategy for global networks; solicited bid: rejected US-based technology when informed of export regulations, 2/93.

7. Boeing: one of largest global users of secure communications: advised Boeing didn't want to have to deal with export regulations for meeting needs: continues to buy Racal products to avoid U.S. regulations. Continue to try to sell, but have met with resistance for procurements 10/92. 4/93, 11/93. Volume would be very high as Boeing took delivery of 800 routers in 1993, and our equipment would have 1:1 relationship. Boeing now in another review cycle.

8. GE: has major program in planning to secure global networks: diverse ownership in many locations has GE seeking foreign solutions for global uniformity.

9. Swiss National Justice and Police Department: project to connect all police and court locations in country: advised by NSA that approval would be hard to justify based on fact that it was Switzerland, 4/94.

10. Thomsen CSF: seeking technology partner for next generation of Thomsen products: sought out Semaphore as Thomsen technology group finds our technology to be far ahead of any other global options, and wanted to have fast time-to-market: NSA suggested we discontinue further discussions, 4/94.

11.Sikorsky: advised permission would not be granted for equipment at foreign joint-venture partners for new commercial helicopter venture, 3/94. Revisited with another NSA export official in 4/94, and advised that license might be granted if use was to principal benefit of a USA company. No firm commitment until license application is submitted as one location is in Japan.

12. Glaxo Pharmaceutical; world's largest pharmaceutical company has global requirement to secure testing and development data: will seek other solutions as Semaphore cannot deliver to other global locations, 2/94.

13. Pillsbury: has strategy to secure global networks: as owned by UK-based Grand Metropolitan, will seek other solutions which can be shipped to all global locations, 11/93.

The total value for all of these opportunities are estimated to be in the range of $30 to $50 million based on the preliminary estimates of the projects.

You have Semaphore's permission to submit this information with your testimony before the Congress.

Gauging the extent of economic harm industrywide is what is an inherently difficult task because most companies do not want to reveal that sort of information. Consequently what exists, with the exception of statements like that from Semaphore, is mostly anecdotal information. But the accumulation of anecdotal information collected by the SPA paints a picture of three ways in which the export controls on cryptographic products are hurting American high-tech industry.

(1) Loss of business directly related to cryptographic products: First, for many data security companies, every sale is vital, and the loss of contracts smaller than $1 million can often mean the difference between life and death for these companies. The confusion and uncertainty associated with export controls on encryption generate severe problems for small firms, but not as severe as the loss of business they suffer from anti-competitive export controls. Examples abound:

- One U.S. company reported loss of revenues equal to a third of its current total revenues because export controls on DES-based encryption closed off a market when its customer, a foreign government, privatized the function for which the encryption was used, and the U.S. company was not permitted to sell to the private foreign firm. The company estimates it loses millions of dollars a year because it receives substantial orders every month from various European customers but cannot fill them because of export controls.
- One small firm could not sell to a European company because that company sold to clients other than financial institutions (for which export controls grant an exception). Later, the software firm received reports of sales of pirated copies of its software. This constituted the loss of a $400,000 contract for the small U.S. software firm.

- Because of existing export restrictions, an American company recently found itself unable to export a mass market software program that provided encryption using Canadian technology based on a Japanese algorithm. Yet other European and Japanese companies are selling competing products worldwide using the same Canadian technology.
- An SPA member's product manager in Europe reported the likely loss of at least 50% of its business among European financial institutions, defense industries, telecommunications companies, and government agencies if present restrictions on key size are not lifted.
- Yet another SPA member company reported the potential loss of a substantial portion of its international business if it cannot commit to provide DES in its programs.
- A German firm that opened a subsidiary in the U.S. sought a single source encryption software product for both its German and U.S. sites. A U.S. data security firm that bid for the contract lost the business because U.S. export controls required that the German firm would have to wait approximately six months while a license was processed to sell them software with encryption for foreign application. The license could only be for one to three years, the three year license being more expensive. Consequently, the German firm ended up purchasing a DES-based system from another German company, and the U.S. firm lost the business.
- A foreign government selected one software company's data security product as that government's security standard. The company's application to export the DES version was denied, and as a consequence the order was lost. This cost the company a $400,000 order and untold millions in future business.

(2) Loss of business from U.S. companies with international concerns: Second, multinational corporations (MNCs) are a prime source of business in the expanding international market for encryption products. Many U.S.-based firms have foreign subsidiaries or operations that do not meet export requirements. While U.S. products may be competitive in the U.S., many MNCs obtain from foreign sources encryption systems that will be compatible with the company's worldwide operations. Moreover, foreign MNCs cannot rely on the availability of U.S. products and have been known to import foreign cryptography for use in their U.S. operations.

- One U.S. firm reports the loss of business from foreign MNCs that will not integrate the company's products into their U.S. operations because of the export restrictions that would prevent them from being compatible with their domestic operations.
- The Computer Business Equipment Manufacturers Association reports that one of its members was denied an export license and lost a $60 million sale of network controllers and software for encryption of financial transactions when the Western European customer could not ensure that encryption would be limited to financial transactions.

(3) Loss of business where cryptography is part of a system: Third, encryption systems are frequently sold as a component of a larger system. These "leveraged" sales offer encryption as a vital component of a broad system. Yet the encryption feature is the primary feature for determining exportability. Because of the export restrictions, U.S. firms are losing the business not just for the encryption product but for the entire system because of the restrictions on one component of it.

- One data security firm has estimated that export restrictions constrain its market opportunities by two-thirds. Despite its superior system, it has been unable to respond to requests from NATO, the Swedish PTT, and British telecommunications companies because it cannot export the encryption they demand. This has cost the company millions in foregone business.
- One major computer company lost two sales in Western Europe within the last 12 months totaling approximately $80 million because the file and data encryption in the integrated system was not exportable.

One possible solution to the problem of export controls may be for U.S. companies to relocate overseas. Some U.S. firms have considered moving their operations overseas and developing their technology there to avoid U.S. export restrictions. Thus, when a U.S. company with technology that is clearly in demand is kept from exporting that technology, it may be forced to export jobs instead.

How are U.S. citizens and businesses being affected by all this?

The answer to this question is painfully simple. When U.S. industry forgoes the opportunity to produce products that integrate good security practices, such as cryptography, into their products because they cannot export those products to their overseas markets, U.S. users (individuals, companies, and government agencies) are denied access to the basic tools they need to protect their own sensitive information.

The U.S. Government does not have the authority to regulate the use of cryptography within this country. But if through strict control of exports they can deter industry from building products that effectively employ cryptography, then they have achieved a very effective form of internal use control. You and I do not have good cryptography available to us in the word processors and data base management and spreadsheet systems even though there is no law against our use of cryptography. If we want to encrypt our sensitive information, we must search out special products that usually must be used separately from our main workstation applications. This is a very effective form of internal use control, and it makes all levels of U.S. industry vulnerable to foreign and domestic industrial espionage.

And Clipper, as presently being implemented, does nothing to help this problem.

What should Congress do?

In this case, Congress is already doing something! Last November, Representative Maria Cantwell introduced HR 3627, a bill that would shift export control of mass market software products including those with cryptography, for the Department of State to the Department of Commerce, thus allowing them to be treated as normal commodities instead of munitions. This bill should be considered as part of Chairman Gejdenson's overall bill to reform export controls. In the Senate, the Murray-Bennett initiative, S 1846, to reform export controls has a similar objective.

Legislation such as HR 3627 and S 1846 must be passed as soon as possible to balance the national economic interests against those of law enforcement and national security.

SUMMARY

On clipper key escrow

In addition to all the concerns about civil liberties and the use of classified cryptography to protect unclassified information, there are very real concerns about whether Clipper will really help law enforcement deal with the emergence of encrypted phone and data traffic. The Administration needs to come forth with some form of business plan for how it expects this program to succeed in the marketplace.

The imposition of a technology as potentially invasive of Americans' right to privacy should not occur merely by executive edict but rather as the result of careful consideration and passage of legislation by the Congress and by being signed into law by the President and determined to be Constitutional by the Supreme Court. Only when this has been completed will most Americans accept key escrow. Only then will Clipper key escrow have a chance of succeeding.

If the Administration does not take immediate steps to introduce legislation defining the role of key escrow in the U.S., Congress must take decisive steps to do so itself.

The digital signature standard

The continuing failure of the U.S. Government to promulgate a Digital Signature Standard after twelve years of trying is a national economic tragedy. The world of electronic commerce could have been well along by now instead ofjust getting started had a standard been established even a few years ago. Those in government who think they are making great strides with the National Performance Review and the National Information Infrastructure will soon realize that until there is an effective DSS, their efforts will be of very limited success.

Make no mistake about it, the reason we have no DSS is because the national security and law enforcement interests in the U.S. have stymied all attempts to approve the logical worldwide defacto standard, and they have not been able to come up with an alternative. And it does not appear that they will succeed in identifying one any time in the near future.

Congress is well justified in taking the extraordinary step of naming a Digital Signature Standard based on the worldwide commercial choice. Congress has an obligation to the American people to allow the U.S. to enter the world of electronic commerce before the 21st century. It truly appears that we may never have a DSS otherwise.

On export control of cryptography

The widespread availability of cryptography throughout the world and the ease with which other countries, including our closest allies, allow the export of cryptography to the U.S. and elsewhere make it imperative that our U.S. Government's regulation of cryptographic exports move out of the Cold War. Export controls have been relaxed on every other form of high tech computer and communications technology. Continuation of cryptography export controls is only hurting American citizens and businesses.

Law enforcement and national security interests will continue to encounter ever-growing amounts of encrypted communications no matter how many restrictive steps the Administration attempts to take. We must realize this basic fact of technology advancement and stop hamstringing U.S. national economic interests in the hope that we are helping our national security interests.

It is evident from the Administration's refusal to relax cryptographic export policies during the Clipper Interagency Review that the Executive Branch is going to continue to emphasize the interests of national security and law enforcement over our national economic interests until we become a third-rate economic power.

Only the Congress can take the steps to balance the interests of American citizens and businesses against that immovable force. I strongly support the Cantwell Bill, HR 3627, and the Murray-Bennett initiative, S 1846.

On a national policy on cryptography

All of these concerns reflect the dilemma between the interests of private citizens and businesses in the U.S. to protect their sensitive information and the interests of law enforcement and national security to be able to monitor the communications of our adversaries.

We need a national statement of policy in this country defining what "rights" individuals and the government can expect in the use of cryptography. Such a policy might ban the use of cryptography by private citizens or remove all restrictions on cryptography exports. More likely, it will seek a compromise to balance our national economic and security interests. One example of such policy is:

> "Good cryptography" shall be available to U.S. citizens and businesses without government restriction.
>
> "Good cryptography" is defined as that which is commonly available throughout the world, presently the Data Encryption Standard and RSA public key cryptography with a 1024-bit modulus.
>
> "Without government restriction" means without export control or other government regulation.

The Administration must understand that until a fair and open review of such a national policy is completed, the struggle over the control of cryptography will not go away.

The Congress can and must play a pivotal role in resolving this dilemma. I strongly urge members of Congress to find a resolution of this issue before our economic interests are surrendered in the interests of law enforcement and national security.

Product	Company	Country	Type	Encrypto	Embodiment	DES
RSA chip	CNET		HW	GENERAL	CHIP	No
RSA chip	Queen's University		HW		CHIP	No
DSD 9812 Data Security Device	Newnet S A	ARGENTINA	HW	GENERAL	CHIP	Yes
DES32 v1 02	Cybenim Pty Ltd.	AUSTRALIA	SW	GENERAL	KIT	Yes
DESF v1 4	Cybenim Pty Ltd.	AUSTRALIA	SW	GENERAL	PGM	Yes
LUC 3 03	Cybenim Pty Ltd.	AUSTRALIA	SW	GENERAL	PGM/KIT	No
SAFA v2 0	Cybenim Pty Ltd	AUSTRALIA	SW	GENERAL	PGM/KIT	No
ERA 2007 Line Encryptor	Erecom Pty Ltd.	AUSTRALIA	HW	COMMS	BOX	Yes
ERA 4007 Line Encryptor	Erecom Pty Ltd	AUSTRALIA	HW	COMMS	BOX	Yes
Erecom Security Module (ESM)	Erecom Pty Ltd.	AUSTRALIA	HW	COMMS	BOX	Yes
Micro Channel Slave Encryptor (MCSE-16)	Erecom Pty Ltd.	AUSTRALIA	HW	GENERAL	BOARD	Yes
Micro Channel Slave Encryptor (MCSE-8)	Erecom Pty Ltd.	AUSTRALIA	HW	GENERAL	BOARD	Yes
PC Encryptor (PCE-16)	Erecom Pty Ltd.	AUSTRALIA	HW	GENERAL	BOARD	Yes
PC Encryptor (PCE 8)	Erecom Pty Ltd.	AUSTRALIA	HW	FILE	BOARD	Yes
ProtectSNA	Erecom Pty Ltd.	AUSTRALIA	SW/HW	COMMS	BOARD	Yes
Secure Access System Software (SAS)	Erecom Pty Ltd.	AUSTRALIA	SW	FILE	PGM	Yes
Series 90 ESM	Erecom Pty Ltd.	AUSTRALIA	HW	COMMS	BOX	Yes
Windows Application Security Program (WASP)	Erecom Pty Ltd.	AUSTRALIA	SW	FILE	PGM	Yes
Icrypt	Eric Young	AUSTRALIA	SW	FILE	PGM	Yes
libdes	Eric Young	AUSTRALIA	SW	GENERAL	KIT	Yes
N-Sure Access 1000	News Datacom	AUSTRALIA	HW	COMMS, DISK	BOARD	Yes
FAXSAFE	Randata	AUSTRALIA	HW	FAX, VOICE	BOX	No
GSA 1000 Duplex Mini Scrambler	Randata	AUSTRALIA	HW	VOICE	BOARD	No
GSA 1300	Randata	AUSTRALIA	HW	VOICE	BOARD	No
Guardian E Data Encryptor	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
Guardian EM Encryptor Modem	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
Guardian EMP Data Encryptor	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
Guardian-EP Data Encryptor	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
Megacrypt High Speed Data Encryptor	Randata	AUSTRALIA	HW			Yes
RD185 Fax	Randata	AUSTRALIA	HW	FAX	BOX	No
RD187 Data Encryptor	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
SecurLAN Network Encryption Unit - Router (NEU-RT)	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
SecurPAC EM Encryptor Modem	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
SecurPac PEM Data Encryptor	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
Securlink Data Encryptor	Randata	AUSTRALIA	HW	COMMS	BOX	Yes
Block-It	Rabvel Software	AUSTRALIA				No
DES Software Toolkit	Cryptech NV/SA	BELGIUM	SW	FILE	KIT	Yes
DES-CHIP	Cryptech NV/SA	BELGIUM	HW	GENERAL	CHIP	Yes
PC-Crypto Toolkit	Cryptech NV/SA	BELGIUM	HW	GENERAL	BOARD	Yes
PC-RSA Processor	Cryptech NV/SA	BELGIUM	HW	GENERAL	BOARD	No
RSA Processor	Cryptech NV/SA	BELGIUM	HW	GENERAL	BOARD	No
MARTLET	GSA Ran Data Europe	BELGIUM				No
Fileguard	Highware, Inc.	BELGIUM		FILE	PGM	No
ISAC 1100	Isolation Systems	CANADA	HW	COMMS, DISK	BOARD	Yes
ISAC 1500	Isolation Systems	CANADA	SW/HW	COMMS, DISK	BOARD	Yes
ISAC 2200	Isolation Systems	CANADA	HW	COMMS, DISK	BOARD	Yes
ISAC 2400	Isolation Systems	CANADA	HW	COMMS, DISK	BOARD	Yes
ISAC 2500	Isolation Systems	CANADA	HW	COMMS, DISK	BOARD	Yes
ISAC 3200	Isolation Systems	CANADA	HW	COMMS, DISK	BOARD	Yes
ISAC 3600	Isolation Systems	CANADA	HW	COMMS, DISK	BOARD	Yes
ISAC 4200	Isolation Systems	CANADA	HW	COMMS, DISK	BOARD	Yes
ISE 2100	Isolation Systems	CANADA	HW	COMMS	BOARD	Yes
FaxSecrets	Mobius Encryption Technologies	CANADA	HW	FAX	BOX	No
TradeSecrets 1000	Mobius Encryption Technologies	CANADA	HW	FILE	BOARD	Yes
TradeSecrets 2000	Mobius Encryption Technologies	CANADA	HW	FILE	BOARD	Yes

ATTACHMENT 1

FOREIGN ENCRYPTION PRODUCTS IDENTIFIED AS OF APRIL 22, 1994

Product	Company	Country	Type	Encrypts	Embodiment	DES
CA20C03A	Newbridge Microsystems	CANADA	HW	GENERAL	CHIP	Yes
Packet Data Security Overlay (PDSO)	Northern Telecom Canada Limited	CANADA	HW	COMMS	BOX	Yes
Data Encryption Board (DEB)	Obiok Data	CANADA	HW	FILE	BOARD	Yes
FAS PACK	Obiok Data	CANADA	SW	FILE COMMS	PGM	Yes
RACAL 3 0	Obiok Data	CANADA	SW/HW	FILE	PGM/BOARD	Yes
RACAL 8 3 0	Obiok Data	CANADA	SW/HW	FILE	PGM/BOARD	Yes
PCMCIA	Secured Communication Canada 93 Inc.	CANADA	HW	FILE	PCMCIA	Yes
Session Key	Secured Communication Canada 93 Inc.	CANADA	HW	GENERAL	PCMCIA	Yes
VICTOR	Aarhus University, Computer Science Department	DENMARK	HW	GENERAL	CHIP	No
6303 SIS	Cryptomathic	DENMARK	SW	GENERAL	PGM	No
8051 DES	Cryptomathic	DENMARK	SW	GENERAL	PGM	Yes
DES Kernel	Cryptomathic	DENMARK	SW	GENERAL	KIT/PGM	Yes
DES Security Mechanisms	Cryptomathic	DENMARK	SW	GENERAL	KIT	Yes
DSP 56000 DES	Cryptomathic	DENMARK	SW	GENERAL	PGM	Yes
DSP 56000 RSA	Cryptomathic	DENMARK	SW	GENERAL	PGM	No
F2F (File-to-File)	Cryptomathic	DENMARK	SW	FILE	PGM	Yes
FRAS File RSA	Cryptomathic	DENMARK	SW	FILE	PGM	No
Multiprecision Kernel	Cryptomathic	DENMARK	HW	GENERAL	KIT	No
PIC16C57 SIS	Cryptomathic	DENMARK	SW	GENERAL	PGM	No
RSA Security Mechanisms	Cryptomathic	DENMARK	SW	GENERAL	KIT	No
safeMatic Security Module	GN Detacom	DENMARK	HW	COMMS	BOX	Yes
DATACO LSA4043 2030025402	LSI Logic/Datoco AS	DENMARK	HW	GENERAL	CHIP	Yes
Datoco LSA4043 2030025402	LSI Logic/Datoco AS	DENMARK	HW	GENERAL	CHIP	Yes
AloDES	Antti Louko	FINLAND	SW	GENERAL	PGM/KIT	Yes
RSA chip	Digital Equipment Corp. (DEC) Paris Research Lab	FRANCE	HW		CHIP	No
RSA Implementations	LAAS	FRANCE				No
P83C852 Smart Card Crypto Controller	Philips Communication Systems	FRANCE	HW	GENERAL	CHIP	No
Crypt II	Real Electronics	FRANCE				No
Very Smart Disk	Smart Diskette	FRANCE	HW	FILE	CARD	Yes
CryptCard	CE Infosys GmbH	GERMANY	HW	GENERAL	PCMCIA	Yes
MiniCrypt	CE Infosys GmbH	GERMANY	HW	GENERAL	BOARD	Yes
SCB810 AT Design Kit	CE Infosys GmbH	GERMANY	HW	GENERAL	BOARD	Yes
SCB820 MCA Design Kit	CE Infosys GmbH	GERMANY	HW	GENERAL	BOARD	Yes
SoftCrypt	CE Infosys GmbH	GERMANY	SW	FILE	PGM	Yes
SuperCrypt	CE Infosys GmbH	GERMANY	HW	GENERAL	CHIP	Yes
cryptLine Controller	CE Infosys GmbH	GERMANY	HW	DISK	BOARD	Yes
ENCRYPT IT v3.08	DataSafe	GERMANY	SW	FILE	PGM	No
WINDEXI v2 01 for DOS	DataSafe	GERMANY	SW	FILE	PGM	No
WINDEXI v2 01 for Windows	DataSafe	GERMANY	SW	FILE	PGM	No
SecuDE PEM	GMD	GERMANY	SW	EMAIL	PGM	Yes
SecuDE 4 2 (Security Development Environment)	GMD	GERMANY	SW	GENERAL	KIT	Yes
TST 3010 High Performance MR Spec Cipher Terminal	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS,TELEX	BOX MODULE	No
TST 3550 Handy Crypt	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS	BOX	No
TST 3570 Packetcrypt	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS	BOX	No
TST 3677 VDU/Screen-Oriented Headquarter Cipher	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS	BOX	No
TST 4043 HF Slow Speed Modem with encryption	Tele Security Timmann GmbH & Co.	GERMANY	HW	FILE, COMMS, FAX	BOX	No
TST 4045 HF Modem 2 4Kbps with encryption	Tele Security Timmann GmbH & Co.	GERMANY	HW	FILE, COMMS, FAX	BOX	No
TST 8500 Crypto Modem	Tele Security Timmann GmbH & Co.	GERMANY	SW/HW	FILE, COMMS, FAX	BOX	No
TST 8580 DataCipher Set	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS, FILE	BOX	No
TST 8583 C Data Encryptor	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS, FILE, FAX	BOX	No
TST 8583 F/C	Tele Security Timmann GmbH & Co.	GERMANY	HW	FAX		No
TST 8583 H/C	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS	BOX	No
TST 8583 N/C	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS	BOX	No
TST 8583 X/C	Tele Security Timmann GmbH & Co.	GERMANY	HW	COMMS	BOX	No
TST 7506 HF voice encryption	Tele Security Timmann GmbH & Co.	GERMANY	HW	VOICE	BOX	No

Product	Company	Country	Type	Encrypts	Embodiment	DES
TST 7610 Secure Office Telephone	Tele Security Timmann GmbH & Co.	GERMANY	HW	VOICE	BOX	No
TST 7698 Miniature Military Voice Coder	Tele Security Timmann GmbH & Co.	GERMANY	HW	VOICE	BOX	No
TST 7700 Telephone Vocoder and Modem	Tele Security Timmann GmbH & Co	GERMANY	HW	VOICE	BOX	No
TST 8010 Spreadspectrum Radio	Tele Security Timmann GmbH & Co	GERMANY	HW	VOICE, COMMS	BOARD	No
TST 8098 Telex Cipher Module	Tele Security Timmann GmbH & Co	GERMANY	HW	COMMS	BOARD	No
TST 8700 INMARSAT "C" encryptor	Tele Security Timmann GmbH & Co	GERMANY	SW/HW	FILE, COMMS, FAX	BOX	No
Disk Encryption Unit	Tulip Computers	GERMANY				No
BACK-Guard	UTI-MACO GmbH	GERMANY	SW	FILE,DISK	PGM	Yes
C-Crypt	UTI-MACO GmbH	GERMANY	SW	FILE	PGM	Yes
SAFE Board I	UTI-MACO GmbH	GERMANY	HW	DISK	BOARD	No
SAFE Board II	UTI-MACO GmbH	GERMANY	HW	DISK	BOARD	Yes
SAFE Board III	UTI-MACO GmbH	GERMANY	HW	DISK	BOARD	Yes
SAFE-Guard EZ	UTI-MACO GmbH	GERMANY	SW	FILE	PGM	Yes
SAFE-Guard GS/2 3 0	UTI-MACO GmbH	GERMANY	SW	FILE,DISK	PGM	Yes
SAFE-Guard Professional 3 2C	UTI-MACO GmbH	GERMANY	SW	FILE,DISK	PGM	Yes
SIGN-Guard	UTI-MACO GmbH	GERMANY	SW	FILE,EMAIL	PGM	Yes
P-8 Security Master Card	Triple D Ltd.	HONG KONG	SW/HW	GENERAL	PGM/BOARD	Yes
Crypte	Chenab Indo Technology	INDIA				No
Descrypt	Eurologic Systems, Ltd.	IRELAND	HW	TAPE	BOX	No
AR Crypto3270-E	Algorithmic Research Ltd.	ISRAEL	SW	COMMS	PGM	Yes
AR Crypto3270 P	Algorithmic Research Ltd.	ISRAEL	SW/HW	COMMS	PGM	Yes
AR CryptoBIOS	Algorithmic Research Ltd	ISRAEL	SW	GENERAL	PGM	Yes
AR CryptoCODE	Algorithmic Research Ltd.	ISRAEL	SW/HW	PIN	PGM/BOARD	Yes
AR CryptoCOM	Algorithmic Research Ltd	ISRAEL	SW	EMAIL	PGM	Yes
AR CryptoMAIN	Algorithmic Research Ltd	ISRAEL	SW	GENERAL	PGM	Yes
AR CryptoPAD	Algorithmic Research Ltd.	ISRAEL	HW	GENERAL	BOX	Yes
AR CryptoPC	Algorithmic Research Ltd.	ISRAEL	SW	GENERAL	PGM	Yes
AR CryptoSAT	Algorithmic Research Ltd.	ISRAEL	HW	TV	BOX	Yes
AR CryptoSafe	Algorithmic Research Ltd.	ISRAEL	HW	GENERAL	BOARD	Yes
AR DISKrete	Algorithmic Research Ltd.	ISRAEL	SW	FILE, DISK	PGM	Yes
FJPEW ver 1 0	Fujitsu Labs Ltd.	JAPAN	SW	EMAIL	PGM	Yes
KPS L1CARD	Yokohama National University	JAPAN				No
UltraCompressor II	Ad Infinitum Programs (AIP-NL)	NETHERLANDS	SW	FILE	PGM	Yes
DEA Crypto Toolkit	Concord Eracom Nederland BV	NETHERLANDS	SW	GENERAL	KIT	Yes
Multi-Functional PC Security (MFPS) Card	Concord Eracom Nederland BV	NETHERLANDS	HW	GENERAL	BOARD	Yes
SCORE	Concord Eracom Nederland BV	NETHERLANDS	SW	GENERAL	KIT	Yes
SECNET (FCM)	Concord Eracom Nederland BV	NETHERLANDS	SW/HW	DISK		Yes
SECNET (HCM)	Concord Eracom Nederland BV	NETHERLANDS	HW	DISK	BOARD	Yes
SECNET (SCM)	Concord Eracom Nederland BV	NETHERLANDS	SW	DISK	PGM	Yes
SECNET FBI-Encryptor	Concord Eracom Nederland BV	NETHERLANDS	HW	GENERAL	BOARD	Yes
SECNET MFPS	Concord Eracom Nederland BV	NETHERLANDS	SW/HW	DISK,COMMS	PGM/BOARD	Yes
SECNET PC Soft-Lock	Concord Eracom Nederland BV	NETHERLANDS				No
Electronic cash systems	DigiCash	NETHERLANDS				No
Electronic toll payment systems	DigiCash	NETHERLANDS				No
Krypter Board	DigiCash	NETHERLANDS	SW/HW	COMMS	BOARD	Yes
AUTHORIZER	Incas Datacom BV	NETHERLANDS	HW	COMMS	BOX	No
SecurIO	Verspeck & Boekers b.v.	NETHERLANDS	HW	COMMS	BOARD	Yes
SecurIO I	Verspeck & Boekers b.v.	NETHERLANDS	HW	COMMS	BOX	Yes
SecurIO II	Verspeck & Boekers b.v.	NETHERLANDS	HW	COMMS	BOX	No
SecurIO III	Verspeck & Boekers b.v.	NETHERLANDS	HW	COMMS	BOX	Yes
LUC Implementation	LUC Encryption Technology, Ltd. (LUCENT)	NEW ZEALAND	SW	GENERAL	KIT	No
HPACK Archiver	Peter Gutmann	NEW ZEALAND	SW	FILE	PGM	No
Cryptos	Aslut	RUSSIA	SW	FILE	PGM	Yes
Absolute Cryptographer	DKL Ltd., Moscow Department	RUSSIA	SW	GENERAL	PGM	No
Excellence for DOS	Elisa Ltd.	RUSSIA	SW	FILE	PGM	No

Product	Company	Country	Type	Encrypts	Embodiment	DES
ATHENA	LAN Crypto	RUSSIA	SW	KEYS		No
VESTA-1	LAN Crypto	RUSSIA	SW	DISK/FILE	PGM	Yes
VESTA 2	LAN Crypto	RUSSIA	SW	DISK/FILE	PGM	Yes
Kryptron	ScanTech	RUSSIA	HW		BOARD	No
TELECRYPT	TELECRYPT, Ltd.	RUSSIA	SW	FILE	PGM	Yes
WATCH	Infoplan - Division of Denel P/L	SOUTH AFRICA	SW		PGM	No
SESAM	Siemens Ltd	SOUTH AFRICA				No
N3000M	Technelics	SOUTH AFRICA				No
SLF 2000	Addy Electronics	SWEDEN	HW	FAX		No
SLP 2000	Addy Electronics	SWEDEN	HW	VOICE		No
SLD/OUS 200	Addy Elektronics	SWEDEN	HW	COMMS	BOX	No
COST Development Tools (GSL/SCL)	COST Computer Security Technologies International	SWEDEN	SW	GENERAL	PGM	Yes
COST EDI	COST Computer Security Technologies International	SWEDEN	SW	COMMS		Yes
COST LAN	COST Computer Security Technologies International	SWEDEN	SW	FILE,COMMS		Yes
COST PEM	COST Computer Security Technologies International	SWEDEN	SW	EMAIL	PGM	Yes
COST SC	COST Computer Security Technologies International	SWEDEN	SW/HW	FILE	TOKEN	Yes
BoKS 4 1 X	DynaSoft	SWEDEN	SW/HW	COMMS	PGM	Yes
HR&S	SONNOR Crypto AB	SWEDEN	SW	FILE, COMMS	PGM	No
PCrypt	SONNOR Crypto AB	SWEDEN	SW	FILE	PGM	No
SecuriCrypto V 24	SecuriCrypto AB	SWEDEN	HW	COMMS	BOX	No
SecuriCrypto V 248	SecuriCrypto AB	SWEDEN	HW	COMMS	BOX	No
SecuriCrypto V 35	SecuriCrypto AB	SWEDEN	HW	COMMS	BOX	No
SecuriCrypto V 38	SecuriCrypto AB	SWEDEN	HW	COMMS	BOX	No
SecuriCrypto X 21	SecuriCrypto AB	SWEDEN	HW	COMMS	BOX	No
SecuriCrypto X 25	SecuriCrypto AB	SWEDEN	HW	COMMS	BOX	No
SecuriCrypto X 28	SecuriCrypto AB	SWEDEN	HW	COMMS	BOX	No
SecuriFax	SecuriCrypto AB	SWEDEN	HW	FAX	CARD	No
SecuriVoice	SecuriCrypto AB	SWEDEN	HW	VOICE	CARD	No
X 25 Advanced Key System	SecuriCrypto AB	SWEDEN	HW	VOICE	BOX	No
DES Implementation 2 2	Stig Ostholm	SWEDEN	SW	GENERAL	PGM	Yes
VINCI	ASCOM Tech AG	SWITZERLAND	HW	GENERAL	CHIP	No
Gretacoder 519	Gretag Data Systems AG	SWITZERLAND	HW	FAX	BOX	No
Gretacoder 522	Gretag Data Systems AG	SWITZERLAND	HW	COMMS	BOX	Yes
Gretacoder 524	Gretag Data Systems AG	SWITZERLAND	HW	COMMS	BOX	Yes
Gretacoder 528	Gretag Data Systems AG	SWITZERLAND	HW	COMMS	BOX	Yes
Gretacoder 545	Gretag Data Systems AG	SWITZERLAND	HW	COMMS	BOX	Yes
Gretacoder 808	Gretag Data Systems AG	SWITZERLAND	HW	COMMS	BOX	Yes
Gretacoder 705 Authenticator	Gretag Data Systems AG	SWITZERLAND	HW	GENERAL	BOX	Yes
Gretacoder 710 Authenticator	Gretag Data Systems AG	SWITZERLAND	HW	GENERAL	BOX	Yes
I-1100	Into Guard AG	SWITZERLAND	HW	COMMS	BOARD	Yes
I-1200	Into Guard AG	SWITZERLAND	SW/HW	GENERAL	KIT BOARD	Yes
I-1200 DES Software	Into Guard AG	SWITZERLAND	SW	GENERAL	KIT	Yes
I-2010	Into Guard AG	SWITZERLAND	HW	COMMS	BOX	Yes
I-3010	Into Guard AG	SWITZERLAND	HW	COMMS	BOX	No
Omnisec 211	Omnisec AG	SWITZERLAND	HW	COMMS	BOX PHONE	No
Omnisec 510	Omnisec AG	SWITZERLAND	HW	COMMS	BOX	No
Omnisec 520	Omnisec AG	SWITZERLAND	HW	FAX	BOX	No
Omnisec 610	Omnisec AG	SWITZERLAND	HW	COMMS	BOX	No
Omnisec 620	Omnisec AG	SWITZERLAND	HW	COMMS	BOX	No
Omnisec 630	Omnisec AG	SWITZERLAND	HW	COMMS	BOX	No
Omnisec 640	Omnisec AG	SWITZERLAND	HW	COMMS	BOX	No
emProtect	Organa	SWITZERLAND				No
PC Guard Professional	Airtech Computer Security	UK				No
RSA chip	British Telecom	UK	HW	GENERAL	CHIP	No
Uerstack	Business Simulations	UK				No

Product	Company	Country	Type	Encrypts	Embodiment	DES
Softlock 10	Compserve Ltd.	UK	SW	FILE	PGM	Yes
X-LOCK 10	Compserve Ltd.	UK	SW	FILE	PGM	Yes
X-LOCK 50	Compserve Ltd.	UK	SW	FILE	PGM	Yes
ACF2	Computer Associates	UK				No
Cortana	Computer Associates	UK				No
Top Secret	Computer Associates	UK				No
Safe Guard Systems	Computer Security Ltd	UK				No
CQ500	Data Innovation Ltd.	UK	HW	COMMS	BOX	Yes
ED2048	Data Innovation Ltd.	UK	HW	VOICE	BOX	Yes
ED500	Data Innovation Ltd.	UK	HW	COMMS	BOX	Yes
ED800	Data Innovation Ltd.	UK	HW	COMMS	BOX	No
ED800R	Data Innovation Ltd.	UK	HW	COMMS	BOX	No
Network Security Workstation (NSW)	Data Innovation Ltd.	UK	SW/HW	KEYS		Yes
PSP400	Data Innovation Ltd	UK	HW	GENERAL	BOARD	Yes
DataCode	DataSoft International Ltd.	UK	SW	GENERAL	KIT	No
DataTalk	DataSoft International Ltd.	UK	SW	COMMS	PGM	No
OS2 IRIS	Digital Crypto	UK	SW	FILE	PGM	Yes
PC IRIS V4.0 - 2	Digital Crypto	UK	SW	FILE	PGM	Yes
PC-MERLIN V2.0 - 1	Digital Crypto	UK	SW	FILE	PGM	Yes
VMS IRIS	Digital Crypto	UK	SW	FILE	PGM	Yes
DATALOK H	GEC-Marconi Secure Systems	UK	HW	COMMS	BOX	No
DATALOK L	GEC-Marconi Secure Systems	UK	HW	COMMS	BOX	No
FAXLOK	GEC-Marconi Secure Systems	UK	HW	FAX	BOX	No
IC-111DSA	GEC-Marconi Secure Systems	UK	HW	VOICE	BOX	No
IC-RP131BSA	GEC-Marconi Secure Systems	UK	HW	VOICE	BOX	No
IC-V200SA	GEC-Marconi Secure Systems	UK	HW	VOICE	BOX	No
MASC	GEC-Marconi Secure Systems	UK	HW	VOICE	BOARD	No
MASC Crypto Management System	GEC-Marconi Secure Systems	UK	SW	KEY	PGM	No
Merocrypt	GEC-Marconi Secure Systems	UK	HW		CHIP	No
SDT-100	GEC-Marconi Secure Systems	UK	HW	VOICE	BOX	No
Safeguard Security System	Global CIS Ltd.	UK	SW	FILE	PGM	No
Secure LAN	IT Security International	UK				No
DataSave-ABA	International Data Security	UK				No
Code-8	J.R. Ward Computes Ltd.	UK	SW	FILE	PGM	No
DataLock CIPHER Procedure	JPY Associates, Ltd.	UK	SW	GENERAL	KIT	Yes
DataLock Editor (DLE)	JPY Associates, Ltd.	UK	SW	FILE, EMAIL	PGM	Yes
DataLock, Version 3.1	JPY Associates, Ltd.	UK	SW	DISK, FILE	PGM	Yes
ZCODA-A	Jaguar Communications Ltd	UK	HW	COMMS	BOX	No
ZCODA-X	Jaguar Communications Ltd.	UK	HW	COMMS	BOX	No
Padlock	Jersa Sovereign	UK				No
CLAM	Micro8 Technology Ltd.	UK	SW	FILE	PGM	No
Trispan	Micronyx UK Ltd.	UK	SW	FILE	PGM,TOKEN	No
Triumphl V2	Micronyx UK Ltd.	UK	SW	FILE	PGM	Yes
Data Delivery/Management System	Network Systems	UK				No
CPS-AuthentCC	PC Security Ltd.	UK	HW	FILE	CARD	No
LapGUARD	PC Security Ltd.	UK	SW	FILE	PGM	No
Stoplock III	PC Security Ltd.	UK	SW	DISK, FILE	PGM	No
Stoplock IV	PC Security Ltd.	UK	SW	DISK, FILE	PGM	Yes
RSA chip	Plessey Crypto	UK	HW		CHIP	No
Policeman	Plus 5 Engineering Ltd.	UK	SW	DISK	PGM	No
Guardian Angel Plus	Protection Systems Ltd.	UK	SW	FILE	PGM	Yes
Datacryptor Key Management Center	Racal-Milgo	UK	HW	COMMS	BOX	No
SAVEDES	S&S International	UK	SW	FILE	PGM	No
DES	Sharewise plc	UK	SW	GENERAL	PGM	Yes
PC-IRIS	Sharewise plc	UK	SW	GENERAL		Yes

Product	Company	Country	Type	Encrypts	Embodiment	DES
PC-Martin	Silververe plc	UK	SW	FILE	PGM	Yes
CRYPTO-JET	Sophos Ltd	UK	HW	FILE	BOARD	Yes
DES Toolkit	Sophos Ltd.	UK	SW	COMMS, FILE	KIT	Yes
EDS	Sophos Ltd	UK	SW	FILE	PGM	Yes
PUBLIC	Sophos Ltd	UK	SW	COMMS	PGM	Yes
RSA Toolkit	Sophos Ltd	UK	SW	GENERAL	KIT	No
SPA Toolkit	Sophos Ltd.	UK	SW	GENERAL	KIT	No
T SAFE	Sophos Ltd.	UK		EMAIL	PGM	No
PS3	Stratford Data	UK				No
Data Jumbler	The Software Forge Ltd	UK	SW	FILE	PGM	Yes
Microstop	Time & Data Systems	UK				No
OSISEC	University College London	UK	SW		PGM	Yes
UK DRA PEM	University College London	UK	SW		PGM	Yes
CP400	Zergo	UK				No
Zetacode A	Zeta Communications Ltd.	UK	HW	COMMS	BOX	No
Zetacode X	Zeta Communications Ltd	UK	HW	COMMS	BOX	No

Company	Product	Type	Encrypts	Embodiment	OES
3Com Corp	LAN Security Architecture (LSA)		COMMS		No
ADT Security Systems	ADT Universal Communicator	HW		CHIP	Yes
AD Electronics	CVAS-III	HW	VOICE		No
AQ Electronics	X-Lock-100	SW/HW	FILE	PCM/BOARD	No
AQ Electronics	X-Lock-50	SW/HW	FILE	CARD	Yes
ASC Systems	Communications Encryption Controller	HW	COMMS		Yes
ASC Systems	DES/COMM	HW			No
ASD Software, Inc	Filegaard	SW	FILE	PCM	No
ASP	Integrity Toolkit				No
AT&T	AT&T Mark E DES Key Generator				Yes
AT&T	AT&T Mark ET DES Key Generator				Yes
AT&T	AT&T Smart Card Version 2 11 / DES	HW	GENERAL	CARD	Yes
AT&T	AT&T Smart Card Version 3.0 / DES (3E1)	HW	GENERAL	CARD	Yes
AT&T	AT&T T7000A Digital Encryption Processor	HW	GENERAL	BOX	Yes
AT&T	Merlin Secure Voice/Data Terminal	HW	COMMS,VOICE	BOX	No
AT&T	STU III Secure Data Device Model 1810	HW	COMMS	BOX	No
AT&T	STU-III Secure Voice/Data Terminal Model 1100	HW	VOICE,COMMS	BOX	No
AT&T	STU-III Secure Voice/Data Terminal Model 2100	HW	VOICE,DATA	BOX	No
AT&T	Secure Data Device 1900	HW	COMMS	BOX	No
AT&T	Surity Facsimile Devices 3700 & 3710	HW	FAX	BOX	Yes
AT&T	Surity Telephone Device 3600	HW	VOICE	BOX	Yes
AT&T	Surity Telephone Device 3600P	HW	VOICE	BOX	No
AT&T	Surity Voice/Data Terminal 4100	HW	VOICE,DATA	BOX	No
AT&T Bell Laboratories	DEP229ER (WE229ER)	HW	GENERAL	BOX	Yes
AT&T Datotek	DKT-1000	HW	COMMS	BOX	No
AT&T Datotek	DLE-7000 Synchronous DataLink Encryptor	HW	COMMS	BOX	No
AT&T Datotek	DNV-2000 Tactical Voice Encryptor	HW	VOICE	BOX	No
AT&T Datotek	DPC-3000 MicroCryptor	HW	FILE		No
AT&T Datotek	XMP-800 Ciphering Message Processor	HW			No
Advanced Computer Security Concepts	Cryptoguard				Yes
Advanced Encryption Systems	Network Security System	HW	COMMS	BOX	Yes
Advanced Micro Devices, Inc (AMD)	AM 9568	HW		BOX	Yes
Advanced Micro Devices, Inc (AMD)	AmZ8068 (also known as the Am9518)	HW		BOX	Yes
Aladdin Software Security	HASP Products				No
American Computer Security	EasyLock	SW	FILE	PCM	Yes
Apple Computer	PowerTalk	SW	COMMS	PCM	No
Applied Software	Data Encryption Facility (DEF)	SW	FILE	PCM	Yes
Arkansas Systems Inc	DES-MATE		COMMS		Yes
Ashton Tate	dBase IV				No
BCC	DES-AT	HW	DISK, COMMS	BOARD	Yes
BCC	SLOT Personal Secure Notebook Computer	HW	DISK		Yes
BLOC Development Corporation	F3 FB (with Security)	SW	FILE	PCM	No
Banyan	Vines				No
Bi-Hex	Cryptex	SW	FILE	PCM	No
Borland	Paradox				No
Brainiree Technology	Scramble		FILE, COMMS		No
Burroughs	2984-9723	HW	GENERAL	CHIP	Yes
Cassidy and Greene	AME (Access Managed Environment) 1.1.3	SW	FILE	PCM	Yes
Cantel Federal Systems	NetAssure	SW/HW	COMMS		Yes
Cantel Federal Systems	NetAssure Server	SW/HW	COMMS		Yes
Cantel Federal Systems	PCAssure 2.4	SW/HW			Yes
Central Point Software	Central Point Backup for DOS/Windows	SW	DISK	PCM	No
Central Point Software	PC Tools Deluxe				No
Certus International	Certus	SW			No
Certtan Corp	SecureModem 2032e	HW	COMMS	BOX	Yes
Certtan Corp	SecureModem 2057e	HW	COMMS	BOX	Yes
Chase Manhasan Bank, N.A.	Chase Enarypton Device 1				Yes

Company	Product	Type	Encrypts	Embodiment	DES
Clarion	Clarion Professional Development				No
Codex Corp	DES4100NSM Network Security Module				No
Codex Corp	MQD88ME DES Chip	HW	GENERAL	CHIP	Yes
Collins Telecommunications Products Division	765 5814-001	HW	GENERAL	CHIP	Yes
Collins Telecommunications Products Division	Voice Privacy Device VP430	HW	VOICE	CHIP	Yes
Command SW Systems	FREEZE 4.0	SW		PGM	Yes
Command SW Systems	FREEZE PLUS 4.0	SW		PGM	Yes
Command SW Systems	LANGUARD	SW		PGM	Yes
Command SW Systems	Security Guardian	SW	FILE	PGM	Yes
Commcrypt	ACCESSGuard	SW		PGM	No
Commcrypt	CryptoLocks	SW	COMMS	PGM	Yes
Communications Devices, Inc	Crypto 817	HW	COMMS	BOX	Yes
Communications Devices, Inc	MultiGuard	SW/HW	PASSWORD	BOX	Yes
Communications Devices, Inc	Orbit	HW	COMMS	BOX	Yes
Communications Devices, Inc	QuadGuard	SW/HW	PASSWORD	BOX	Yes
Complan	DESCIK	SW	FILE	PGM	Yes
Computer Associates International, Inc.	CA ACF2/PC 1.0	SW		PGM	Yes
Computer Associates International, Inc.	CA CORTANA 1.0	SW	FILE	PGM	Yes
Computer Associates International, Inc.	CA-Top Secret/PC 1.0	SW		PGM	Yes
Contemporary Cybernetics	CY-2000	HW	DISK		No
Contemporary Cybernetics	CY-8500-B				No
Crypta8	DPU-1000	HW		BOX	Yes
Crypta8	DPU-1000S	HW		BOX	Yes
Crypta8	DPU-1000X	HW		BOX	Yes
Cryptech	Redac-Cuts	HW	COMMS		No
Cylink Corp.	12422-001, DES2M1CFB				Yes
Cylink Corp.	9100 Network Integrator	HW	COMMS	BOX	Yes
Cylink Corp.	Advanced Smart Card	HW	GENERAL	CARD	No
Cylink Corp.	CIDEC-HS	HW	COMMS	BOX	Yes
Cylink Corp.	CIDEC-HX	HW	COMMS	BOX	No
Cylink Corp.	CIDEC-LS	HW	COMMS	BOX	Yes
Cylink Corp.	CIDEC-LX	HW	COMMS	BOX	No
Cylink Corp.	CIDEC-MLX Central Encryption System	HW	COMMS	BOX	No
Cylink Corp.	CIDEC-MS	HW	COMMS	BOX	Yes
Cylink Corp.	CIDEC-VH	HW	COMMS	BOX	No
Cylink Corp.	CIDEC-VHS	HW	COMMS	BOX	Yes
Cylink Corp.	CKG-VHS Data Encryptor	HW	COMMS	BOX	No
Cylink Corp.	CY 1024	HW	GENERAL	CHIP	No
Cylink Corp.	CY1045	HW		CHIP	Yes
Cylink Corp.	CY512	HW	GENERAL	CHIP	No
Cylink Corp.	Cylink Feades				Yes
Cylink Corp.	FAXLOK	HW	FAX	BOX	No
Cylink Corp.	LS 20 Low Speed Data Encryptor	HW	COMMS	BOX	Yes
Cylink Corp.	LX 20 Low Speed Data Encryptor	HW	COMMS	BOX	No
Cylink Corp.	BTM-9800	HW	VOICE,DATA	BOX	Yes
Cylink Corp.	SecureCELL Secure Cellular Telephone	HW	VOICE	BOX	Yes
Cylink Corp.	SecureCELLX Secure Cellular Telephone	HW	VOICE	BOX	No
Cylink Corp.	SecureFX Standalone FAX Encryptor	HW	FAX	BOX	Yes
Cylink Corp.	SecureFXP Standalone FAX Encryptor	HW	FAX	BOX	No
Cylink Corp.	SecurePC	SW/HW	FILE	PGM/BOARD	Yes
Cylink Corp.	SecurePC/T	SW/HW	FILE	PGM/BOARD	Yes
Cylink Corp.	SecurePhone	HW	VOICE	BOX	Yes
Cypher Comms Technology	CYCOM				No
DSC Communications	Nexus				No
DataEase International	DataEase				No
DataMedia Corporation	SECUREcard Model 100	HW	FILE	TOKEN	Yes
DataMedia Corporation	SECUREcard Model 200	SW	FILE		Yes

Company	Product	Type	Encrypts	Embodiment	DES
DataMedia Corporation	SECUREcard Model 400		FILE	PCM BOARD	Yes
DataMedia Corporation	SECUREexchange	SW	COMMS	PCM	Yes
Datakey Inc.	110-310 ASACS Smart Card	HW		CARD	Yes
Datawatch, Triangle Software Division	Datawatch Citadel with Shredder	SW	FILE	PCM	No
Datawatch, Triangle Software Division	Datawatch Superset Utilities	SW	FILE	PCM	No
Datotek	D U D E.	HW	COMMS		Yes
Datotek	DVC-2418	HW	VOICE	BOX	Yes
Digital Delivery, Inc	CD Product Portfolio	SW		PCM	No
Digital Enterprises	Deadbolt	HW	FILE		Yes
Digital Enterprises	Deadbolt Data/Fax Modem	HW	FAX, COMMS	BOX	No
Digital Enterprises	Netlock	HW	COMMS	CARD	No
Digital Enterprises	Propack	HW	DISK	BOX	No
Digital Enterprises	Shockpack	HW		BOX	No
Digital Equipment Corp (DEC)	VAX Encryption	SW	FILE	PCM	Yes
Digital Equipment Corp (DEC)	VAX KDC System		COMMS		No
Digital Pathways	Defender II	HW	COMMS		Yes
Digital Pathways	SecureNet Key	HW		TOKEN	Yes
Dolphin Software	Dolphin Encrypt	SW	GENERAL	KIT	No
Dolphin Software	Dolphin Encrypt Advanced Version	SW	DISK,FILE	PCM	No
Dolphin Software	EZ-Crypt	SW	DISK	PCM	No
Downy Network Systems	SciNet Data Encryption System	SW/HW	COMMS		Yes
ELIASHIM Microcomputers, Inc.	CodeSafe	SW	DISK	PCM	No
Enigma Logic	SafeWord PC LAN Safe		FILE		No
Enigma Logic	SafeWord PC Safe II	SW	FILE		Yes
Enigma Logic	SafeWord PC Safe III	SW	FILE		Yes
Enigma Logic	SafeWord Terminal Safe		FILE		No
Enterprise Solutions Ltd	ES / Secure	SW	EMAIL	KIT	Yes
Fairchild Semiconductor	9414 Chip Set	HW		CHIP	Yes
Fifth Generation Systems	DiskLock	SW	FILE		Yes
Fifth Generation Systems	DiskLock PC	SW	FILE		Yes
Fischer International	Kryptonite	SW	COMMS, FILE		Yes
Fischer International	MailSafe	SW	COMMS		No
Fischer International	RSA/3270	SW	COMMS	PCM	Yes
Fischer International	SafeBoot	SW	DISK	TOKEN	No
Fischer International	Watchdog Armor	SW/HW	FILE	BOARD	Yes
Fischer International	Watchdog Director	SW	COMMS	PCM	No
Fischer International	Watchdog PC Data Security 6.0	SW	FILE	PCM	Yes
Front Line Software	726-8084 PROM Device	HW	GENERAL	CHIP	Yes
Gemplus Card International	MCO816K EEPROM/DES	HW		CARD	Yes
General Electric Company	19080137S	HW	VOICE	CHIP	Yes
Glenco Engineering	GLEN-DES	HW	GENERAL	CHIP	Yes
Glenco Engineering	HL-Crypt	SW	PROGRAMS	PCM	No
Glenco Engineering	Hardlock 1.01	HW			No
Glenco Engineering	Hardlock-DES	HW	GENERAL	BOX (PER?)	No
HYDELCO Inc.	InfoShield	HW	FILE,COMMS	BOARD	No
Hawkeye Grafix, Inc.	DES-PAC 3.0	SW	FILE		Yes
Hitachi Inc.	Hyper ACCESS /5 Secure	SW	COMMS	PCM	No
Hughes Aircraft Company	NetLOCK	SW	COMMS	PCM	Yes
Hughes Aircraft Company	Shepard	SW	LABELS	PCM	Yes
Hughes Data Systems, Inc.	SECUREPC	SW	FILE		No
Hughes Data Systems, Inc.	SECUREPC PLUS	SW	FILE		No
Hughes Network Systems - California	LC75				Yes
Hughes Network Systems - California	LC76CF				Yes
Hughes Network Systems - Maryland	Integrated Satellite Business Network (ISBN)	SW	COMMS,VOICE,FAX		No
INFOSAFE	X-Lock 10				No
INFOSAFE	X-Bolt 10				No
Information Resource Engineering	Atlas Encryption System		COMMS		No

Company	Product	Type	Encrypts	Embodiment	DES
Information Resource Engineering	Network Security Systems		COMMS, FILE		Yes
Information Security Associates Inc.	SignalGuard				No
Information Security Corp	Crypt Master 3 10	SW	FILE, COMMS	PGM	Yes
Information Security Corp	Secret Agent	SW	FILE	PGM	Yes
Information Security Corp	Secure 2 MODEM	SW	COMMS	PGM	Yes
Information Security Corp	SpyProof	SW	COMMS, DISK	PGM	Yes
Information Security Systems	SecureInfo	HW	FILE	CARD	No
Innovative Communications Technologies Inc	COMSEC Module	HW		BOARD	No
Intel	8294	HW		BOX	Yes
Intel	8294A	HW		BOX	Yes
Inter-Tech Corp	Datamobile II IDE Series	HW	DISK	DISK	No
Inter-Tech Corp	Datamobile II SCSI High Capacity Series	HW	DISK	DISK	No
Inter-Tech Corp	Datamobile II SCSI Slim Profile Series	HW	DISK	DISK	No
International Business Machines (IBM)	4402182	HW	GENERAL	CHIP	Yes
International Business Machines (IBM)	8432242	HW	GENERAL	CHIP	Yes
International Business Machines (IBM)	8678178	HW	GENERAL	CHIP	Yes
International Business Machines (IBM)	IBM 4753 Network Security Processor	HW	COMMS	BOX	Yes
International Business Machines (IBM)	IBM 4754 Security Interface Unit	HW	COMMS	CARD	Yes
International Business Machines (IBM)	IBM 4755 Cryptographic Adapter Card	HW	COMMS	BOARD	Yes
International Business Machines (IBM)	IBM Integrated Cryptographic Feature (ICAF)	HW	COMMS, FILE	BOX	Yes
International Business Machines (IBM)	P/N 8270094 using DES chip P/N 5898057	HW		CHIP	Yes
John E. Holt and Associates	Krypton Firmware	HW	GENERAL	CHIP	Yes
Janes Futures	ENC-300A	HW	GENERAL	BOARD	Yes
Janes Futures	ENC-324	HW	GENERAL	BOARD	Yes
Janes Futures	ENC-328	HW	GENERAL	BOARD	Yes
Janes Futures	ENC-334	HW	GENERAL	BOARD	Yes
Janes Futures	ENC-336	HW	GENERAL	BOARD	Yes
Janes Futures	ENC-400	HW	COMMS	BOX	Yes
Janes Futures	ENC-526	HW	GENERAL	BOARD	Yes
Janes Futures	Protec Plus	SW/HW	FILE, DISK	PGM/BOARD	Yes
Janes Futures	SAFE Vault 300	HW	FAX	BOX	Yes
Janes Futures	SAFE Vault 400	HW	FAX	BOX	No
Kensington Microwere Ltd.	Passproof	SW/HW			Yes
Kent Marsh Ltd	MacSafe II 2 0	SW	FILE		Yes
Key Concepts	SureKey/2	SW			No
Kinetic Corp	Kinetic Encryption 2 0	SW	FILE, DISK		Yes
Lassen Software, Inc.	Trusted Access	SW			No
Lattice Inc.	SecretDisk II	SW	FILE, DISK	PGM	Yes
Lexicon	LEX-POS (Model 800)	HW		BOX	Yes
Libronic Industries	LEAD	HW	FILE, COMMS	CARD	No
Libronic Industries	MPA-100	HW	COMMS	BOX	Yes
Libronic Industries	PCA-100	HW	GENERAL	BOARD	Yes
Libronic Industries	SPA-100	HW	COMMS	BOX	Yes
Lotus	Lotus 123				No
Lotus	Lotus Notes	SW	COMMS	PGM	No
Lotus	cc Mail				No
MCTel	MCTel Security System	SW	GENERAL	PGM	Yes
MaeDae Enterprises	ENCRYPT-IT v2 0 for DOS	SW	FILE	PGM	Yes
MaeDae Enterprises	ENCRYPT-IT v2 0 for Windows	SW	FILE	PGM	Yes
Magna	Empower I 4 0	SW	DISK	PGM	Yes
Magna	Empower II 4 0	SW	FILE, DISK	PGM	Yes
Magna	Empower III 4 0	SW	FILE, DISK	PGM	Yes
Mark Riorden	RIPEM 1 2	SW	FILE,EMAIL	PGM	Yes
Massachusetts Institute of Technology (MIT)	TechMail with PEM	SW	EMAIL	PGM	Yes
Matsushita Electronic Component Co.	EBC 1842 IC Card	HW		CARD	Yes
Mergent International	Net/Data Access Control System				No
Mergent International	PC/DACS 20201	SW	DISK	PGM	Yes

Company	Product	Type	Encrypts	Embodiment	DES
Mergent International	SSO/DACS	SW	FILE	PGM	Yes
Micanopy MicroSystems, Inc.	ZCrypt 1.2	SW	FILE	PGM	No
Micro Card Technologies, Inc	Micro Card TS100 Integrated Circuit Card	HW		CARD	Yes
Micro Security Systems, Inc.	DecurKey	HW	FILE	BOX	Yes
Micro Security Systems, Inc	SECURIDATA	HW	COMMS	CARD	No
MicroFrame, Inc	CipherKEY	HW	COMMS	BOX	Yes
MicroFrame, Inc	DataLOCK 4000	HW	COMMS	BOX	Yes
MicroFrame, Inc	Dataguard 4000	HW	COMMS	BOX	Yes
Microcom, Inc (Utilities Product Group)	Citadel	HW	FILE	BOX	Yes
Microlink Technologies, Inc	MicroCrypt (for UNIX)	SW	FILE		No
Microlink Technologies, Inc	MicroCrypt (for VMS)	SW	FILE		No
Microlink Technologies, Inc	MicroCrypt (for the PC)	SW	FILE	PGM	No
Microlink Technologies, Inc	NetWizard	SW	FILE	PGM	Yes
Micromyx	SAFE	SW	FILE, DISK	PGM	No
Micromyx	Secured DOS	SW	FILE	PGM	No
Micromyx	TRISPAN	SW/HW	FILE	BOARD	No
Micromyx	Triumph 2				No
Micromyx	Triumph1	SW	FILE		Yes
Microrim	R Base				No
Microsoft	Excel				No
Microsoft	LAN Manager 2.0				No
Microsoft	Mail 2.x				No
Microsoft	Mail 3.0 for MAC				No
Microsoft	Word 2.0 for Windows				No
Mike Ingle	Secure Drive 1.1	SW	DISK, FILE	PGM	No
Morning Star Technologies	Morning Star Express Router 2e	HW	COMMS	BOX	Yes
Morning Star Technologies	Morning Star PPP	SW	COMMS	PGM	Yes
Morse Security Group Inc	TRAP 5200 System	HW	COMMS		Yes
Motorola	MC6852	HW		BOX	Yes
Motorola	Network Encryption Systems (NES)				No
Motorola	SECTEL 1500	HW	COMMS,FAX,VOICE	BOX	No
Motorola	SECTEL 2500	HW	COMMS,FAX,VOICE	BOX	No
Motorola	SECTEL 9600	HW	COMMS,FAX,VOICE	BOX	No
Motorola	SECTEL MICRO MMT	HW	VOICE	BOX	No
Motorola	SECTEL MMT 1500	HW	VOICE	BOX	No
Motorola	SECTEL MMT 3500	HW	VOICE	BOX	No
Motorola	TSW-2	HW			Yes
National Semiconductor	iPower	HW	GENERAL	TOKEN	Yes
Network-1, Inc.	Secure Front End (SFE)	SW	COMMS		No
Networking Dynamic Corp.	Compufax	SW	FAX	PGM	No
Nikkori Computer Corporation	VEM Module	HW		BOX	Yes
Norton	Norton Utilities 4.0e				No
Norell	NameService				No
Norell	Netware 386 3.1				No
OnLine SW International	Ramis				No
Optimum Electronics, Inc.	PC PASSKey	SW	DISK	PGM	No
Otacom Systems, Inc.	3298 Secure Communications Center	HW	COMMS,FAX,VOICE	BOX	No
PC Access Control, Inc.	STOPLOCK		GENERAL		Yes
PC Dynamics, Inc.	Total Security	SW	COMMS, FILE	PGM	Yes
PC Guardian	DES Encryption Module	SW	FILE	PGM	Yes
PC Guardian	Encryption Plus	SW	DISK	PGM	No
PC Plus, Inc.	Encrypted CD-ROM Publishing System	SW/HW	CD-ROM	BOX	No
PC Plus, Inc.	Encrypted CD-ROM Publishing System	SW/HW	CD-ROM	BOX	Yes
Paradyne Corporation	InfoLock 1027 Model 2811-03	HW	FILE, COMMS	BOX	Yes
Paradyne Corporation	InfoLock Model 2811-11	HW	FILE, COMMS	BOX	Yes
Persian Technologies	Pathkey	SW/HW	COMMS	TOKEN	Yes
Personal Computer Card Corp.	LapGuard	SW	FILE		Yes

Company	Product	Type	Encrypts	Embodiment	DES
Personal Computer Card Corp	PCSS	SW	FILE	TOKEN	Yes
Pinon Engineering Inc.	CRYPTIE				No
Prime Factors	DESCRYPT & DESCRYPT+	SW	GENERAL	PGM	Yes
Prime Factors	DESCRYPT/BS & DESCCRYPT+/BS	SW	GENERAL	KIT	Yes
Prime Factors	DESCRYPT/C & DESCNYPT+/C	SW	GENERAL	KIT	Yes
Prime Factors	DESCRYPT/CS & DESCRYPT+/CS	SW	GENERAL	KIT	Yes
Prime Factors	DESCRYPT/FS & DESCRYPT+/FS	SW	GENERAL	KIT	Yes
Prime Factors	DESCRYPT/MS	SW	GENERAL	KIT	Yes
Prime Factors	Diogenes	SW	FILE	PGM	Yes
Prime Factors	PIN Management System	SW	COMMS	PGM	Yes
Prime Factors	PINSYS & PINSYS+	SW	COMMS	PGM	Yes
Prime Factors	PSYPHER & PSYPHER+	SW	FILE	PGM	Yes
Prime Factors	PSYPHER/VM	SW	FILE	PGM	Yes
Prime Factors	PSYPHER/VS	SW	FILE	PGM	Yes
Prime Factors	VECTORADES	SW			Yes
Prime Factors	v-PSYPHER	SW	GENERAL	PGM	Yes
RSA Data Security	BSAFE 2.0	SW	GENERAL	KIT	Yes
RSA Data Security	MailSafe 5.0	SW	EMAIL	PGM	Yes
RSA Data Security	RSA/DSP	HW	GENERAL	BOARD	Yes
RSA Data Security	TIPEM	SW	EMAIL	KIT	Yes
RSA Laboratories	RSAREF	SW	EMAIL	KIT	Yes
Racal Datacom	Datacryptor 64	HW	COMMS	BOX	Yes
Racal Datacom	Datacryptor 24 1027	HW	COMMS	BOX	Yes
Racal Guardata	Asynchronous Gateway	HW			Yes
Racal Guardata	CAT 2000, 2001, 2001II	HW	COMMS	CARD	Yes
Racal Guardata	CAT 2080	HW	COMMS	CARD	Yes
Racal Guardata	Gateway Security	HW	COMMS	BOX?	Yes
Racal Guardata	Host Security Module (HCM)	HW	COMMS	BOX	Yes
Racal Guardata	ISM-444	HW	COMMS	BOX	Yes
Racal Guardata	LEAD		COMMS		No
Racal Guardata	Personal Computer Security Module (PCSM)	HW	GENERAL	BOARD	Yes
Racal Guardata	X.28 Gateway	HW	COMMS		Yes
Racal Guardata	X.9 Cryptoserver	HW	COMMS		Yes
Racal Guardata	Datacryptor	HW	GENERAL	BOX	Yes
Racal Milgo USA	Data Sentry	HW	FILE		Yes
Rainbow Technology	DataLock	SW	FILE	PGM	No
Rasco	CLS Series 3200 Encryption Module	HW	COMMS	BOX	Yes
Rothenbuhler Engineering	SecurData		COMMS		No
S Squared Electronics	SCO Unix System V/386				No
SCO	Secure Voice	SW	VOICE	PGM	Yes
SVC	StopLight	SW	FILE	PGM	Yes
Safetynet	Ami Pro				No
Samna Corp.	Scrambler 1.1	SW	FILE	PGM	Yes
Scrambler Systems Corp	Citadel 4.04	SW	FILE	PGM	Yes
Secor Technology	Port of Entry 3.0	SW	FILE	PGM	Yes
Secor Technology	Sentinel 4.04	HW	FILE		Yes
Secor Technology	DESPLEX	HW			Yes
Secur-Data Systems, Inc.	LANSECURE	HW	COMMS	CHIP	No
Secure Technologies	LOCK	SW	FILE	PGM	Yes
Secure Systems Group International, Inc.	LOCK (Hardware version)	HW	FILE		Yes
Secure Systems Group International, Inc.	DesMaster Hardware 1.0	HW	FILE		Yes
Security Microsystems, Inc.	DesMaster Software	SW	FILE	PGM	Yes
Security Microsystems, Inc.	Lockit I Extended Edition 3.0	HW	FILE		Yes
Security Microsystems, Inc.	Lockit III 2.03	SW	FILE	PGM	No
Security Microsystems, Inc.	Lockit Professional 2.14	SW/HW	FILE		Yes
Semaphore Communications	Network Security System		FILE, COMMS		Yes
Sentry Systems, Inc	SENTRY CLASS IV	SW/HW	FILE, DISK	BOARD	Yes

Company	Product	Type	Encrypts	Embodiment	DES
Silver Oak Systems	SeniCad	SW	FILE	PGM	Yes
SmartDisk Security Corp	SafeBoot	SW/HW	DISK	KIT	No
Software Directions, Inc	Softsafe 2.0	SW	FILE	PGM	No
Solid Oak Software	PC-Sentry	SW	FILE	PGM	No
SophCo, Inc.	Osiekeeper				No
SophCo, Inc.	PROTEC 3.5A	SW	FILE	PGM	Yes
SophCo, Inc.	PROTEC Passport				No
SophCo, Inc.	PROTEC Platinum				No
Sota Milispe	PassPort Communications Security System		COMMS		Yes
Stellar Systems, Inc.	EFS 3		VOICE, COMMS		Yes
Stellar Systems, Inc.	Sabrewatch		VOICE, COMMS		Yes
Sterling Software Inc. (Dytekar Division)	DYL-Security		FILE		Yes
Sterling Software Inc. (Sys SW Mktg Div)	Shrink	SW	FILE	PGM	No
SunSoft	SunShield Acct Resource Management				No
SunSoft	SunShield Auto Enh Security Tool				No
Symantec	Q&A 4.0				No
Technar Computer Products, Inc.	COMLOCK	SW	DISK		No
Technar Computer Products, Inc	#ICRYPT	SW	FILE	PGM	No
Technical Communications Corp (TCC)	CSD 3324A	HW	VOICE, COMMS	BOX	Yes
Technical Communications Corp (TCC)	CSD 3324E		COMMS,FAX,VOICE		No
Technical Communications Corp (TCC)	Cipher s850 Digital Encryption System		GENERAL		No
Technical Communications Corp (TCC)	DSP 72A SP Military Bulk Ciphering System		COMMS		No
Technical Communications Corp (TCC)	DSP 9000 Military Ciphering System		VOICE, COMMS		No
Technical Communications Corp (TCC)	KEYNET		COMMS		No
Telequip Corp	Hotline		COMMS		Yes
Terry Ritter	Penknife for DOS	SW	FILE	PGM	No
Texas Instruments, Inc	TMS 99541	HW		CHIP	Yes
The Exchange	EXCRYPT DES 64 KM	HW		BOX	Yes
Thumbscan, Inc.	PCBoot 2.50	HW	FILE		No
Thumbscan, Inc.	SoftBoot 2.50	SW	FILE	PGM	No
Trascar Ultron	Crypto-Engine	HW	GENERAL	CHIP	No
Trascar Ultron	LVSSP3110 Data Storage Encryptor	HW	DISK	BOX	No
Trigram Systems	DES Module	SW	GENERAL	PGM/KIT	Yes
Trigram Systems	DataSafe	SW	FILE, DISK	PGM	Yes
Trilan Systems	CypherInk	HW	COMMS	BOX	Yes
Trusted Information Systems, Inc.	TIS/PEM	SW	EMAIL	PGM	Yes
Trusted Information Systems, Inc	Trusted Mail	SW	EMAIL	PGM	Yes
UNIVAC	End-End / Mass Storage Encryptor	HW			Yes
UUNet Technologies, Inc.	Lan Guardian		COMMS		No
United Software Security	Privacy Plus 3.01	SW	FILE	PGM	Yes
VLSI	VM007 Encryption Processor	HW		CHIP	Yes
VLSI Technology, Inc.	VM008 Data Encryption Processor	HW		CHIP	Yes
Verdix Corp (Secure Product Division)	VSLAN	HW	COMMS		Yes
VisCrypt	DigiSign 150	SW	GENERAL	KIT	Yes
VisCrypt	DigiSign 360	SW/HW	GENERAL	KIT/ BOX	Yes
VisCrypt	DigiSign 380	SW/HW	GENERAL	KIT/BOARD	Yes
VisCrypt	DigiSign D360	SW/HW	GENERAL	KIT/BOX	Yes
VisCrypt	VisCrypt PGP for MS-DOS Version 2.4	SW	FILE, EMAIL	PGM	No
VisCrypt	VisCrypt PGP for UNIX Version 2.4	SW	FILE, EMAIL	PGM	No
VisCrypt	VisCrypt PGP for WnCIM/CSNav Version 2.4	SW	FILE, EMAIL	PGM	No
Visionary Electronics	Visionary 2400XT	HW	COMMS	BOX	No
Wang Laboratories	Trusted Interface Unit (TIU)	HW	COMMS	BOX	No
Wells Fargo Security Products	WP PN 5296 / WP PN 5297	HW		CHIP	Yes
Western DataCom Co. Inc.	434 CryptoCard	HW	COMMS	CARD	Yes
Western DataCom Co. Inc.	432 CryptoCard	HW	COMMS	CARD	Yes
Western DataCom Co. Inc.	764 CryptoPress	HW	COMMS	BOARD	Yes
Western DataCom Co. Inc.	625 CryptoNet	HW	COMMS	BOX	Yes

Company	Product	Type	Encrypte	Embodiment	DES
Western DataCom Co Inc.	Line Guard 8000	HW	COMMS	BOX	Yes
Western DataCom Co Inc	MESA 424	HW	COMMS	BOX	Yes
Western DataCom Co Inc	MESA 432	HW	COMMS	BOX	Yes
Western DataCom Co Inc	MESA 4321	HW	COMMS	BOARD	Yes
Western Digest Corporation	WD 2002 / WD 2012	HW		BOX	Yes
Western Digest Corporation	WD20C03 DES Device	HW		BOX	Yes
WordPerfect	WordPerfect				No
WordPerfect	WordPerfect Office				No
X Tree	X Tree Net 2 0				No
Xetron Corporation	Macintosh Software Media Encryption (MSME)	SW	FILE	PGM	No
Xetron Corporation	PC Software Media Encryption (PSME)	SW	FILE	PGM	No
Yeargin Engineering	HyperCrypt 1 1				No
hDC	NDC FileAppe				No
uwEZ Software Inc.	CamouFlage	SW	DISK, COMMS	PGM	No
uwEZ Software Inc	UltraSHIELD	SW	FILE	PGM	No

ATTACHMENT 2
COMPANIES MANUFACTURING AND/OR DISTRIBUTING CRYPTOGRAPHIC PRODUCTS WORLDWIDE

From the Software Publishers Association survey of cryptographic products as of April 25, 1994.

ARGENTINA	Newnet S.A.
AUSTRALIA	Cybanim Pty Ltd. Datamatic Pty Ltd. Eracom Pty Ltd. Eric Young Loadplan Australasia Pty Ltd. LUCENT News Datacom Randata Robust Software Ross Williams Sagem Australasia Pty Ltd. TRAC Systems Tracom
AUSTRIA	Schrack-Dat
BAHRAIN	International Information Systems
BELGIUM	Cryptech NV/SA GSA Ran Data Europe Highware, Inc. Unina SA Vector
CANADA	A.B. Data Sales, Inc. Concord-Eracom Computer Ltd. Isolation Systems Mobius Encryption Technologies Newbridge Microsystems Northern Telecom Canada Limited Okiok Data Paradyne Canada Ltd.

	Secured Communication Canada 93, Inc.
DENMARK	Aarhus University, Computer Science Department CryptoMathic GN Datacom Iversen & Martens A/S LSI Logic/Dataco AS Swanholm Computing A/S
FINLAND	Antti Louko Ascom Fintel OY Instrumentoiti OY
FRANCE	Atlantis CCETT CSEE - Division Communication et Informatique CSIL Cryptech France Dassault Automatismes et Telecommunications Digital Equipment Corporation (DEC), Paris Research Lab Incaa France S.A.R.L. LAAS Philips Communication Systems Rast Electronics S.A. Gretag Sagem Smart Diskette Societe Sagem
GERMANY	AR Datensicherungssysteme GmbH CCI CE Infosys GmbH Concord-Eracom Computer GmbH Controlware GmbH Data Safe Dynatech-Gesellschaft fur Datenverarbeitung GmbH EuroCom EDV FAST Electronic Gliss & Herweg GMD Gretag Elektronik GmbH

	KryptoKom
	Markt & Technik Software Partners Intl. GmbH
	Paradyne GmbH
	Siemens
	Smart Diskette GmbH
	Tela Versicherung
	Tele Security Timmann
	Telenet Kommunication
	The Compatibility Box GmbH
	Tulip Computers
	UTI-MACO GmbH
GREECE	G.J.Messaritis & Co. Ltd.
	ORCO Ltd.
HONG KONG	News Datacom
	Triple D Ltd.
INDIA	Chenab Info Technology
IRELAND	Eurologic Systems, Ltd.
	Renaissance Contingency Services, Ltd.
	Shamus Software Ltd.
ISRAEL	Algorithmic Research Ltd.
	ELYASIM
	News Datacom
	TADIRAN
ITALY	Incaa SRL
	Olivetti
	Ratio Srl
	Telvox s.a.s.
	Uniautomation
JAPAN	Fujitsu Labs Ltd.
	Japan's National Defense Academy
	Paradyne Japan, KK
	Yokohama National University
LUXEMBORG	Telindus SA
MALTA	Shireburn Co. Ltd.

NETHERLANDS	Ad Infinitum Programs (AIP-NL) CRYPSYS Data Security Concord Eracom Nederland BV Cryptech Nederland DigiCash DSP International Geveke Electronics BV Incaa Datacom BV Incaa Nederland BV Repko BV Datacomms Verspeck & Soeters BV
NEW ZEALAND	LUC Encryption Technology, Ltd. (LUCENT) Peter Gutmann Peter Smith and Michael Lennon
NORWAY	BDC Bergen Data Consulting A/S Ericcson Semafor PDI Scand PC Sys/Sectra Skanditek A/S UMI SA
POLAND	SOFT-u.1.
PORTUGAL	Infornova Redislogar SA
RUSSIA	Askri DKL Ltd. Elias Ltd. LAN Crypto RESCrypto ScanTech TELECRYPT, Ltd.
SAUDI ARABIA	Info Guard Saudi Arabia
SINGAPORE	Communications Systems Engineering Pty. Ltd. Digitus Computer Systems
SOUTH AFRICA	BSS (Pty) Ltd. Computer Security Associates

	EFT
	InfoPlan - Division of Denel P/L
	Intelligent
	Nanoteq
	Net One
	Siemens Ltd.
	Spescom
	Technetics
SPAIN	Asociacion Espanola de Empresas de Informatica
	Asociacion Nacional de Industrias Electronicas
	Redislogar Comminicaciones SA
	SECARTYS
	Sinutec
	Tecnitrade Int. SA
SWEDEN	AV System Infocard
	Ardy Elektronics
	Au-System Infocard AB
	COST Computer Security Technologies
	International
	DynaSoft
	QA Informatik AB
	SONOR Crypto AB
	SecuriCrypto AB
	Stig Ostholm
	Tomas Tesch AB
SWITZERLAND	ASCOM Tech AG
	Brown-Boveri
	Crypto AG
	ETH Zurich
	Ete-Hager AG
	Gretag AG
	Incaa Datacom AG
	Info Guard AG
	Omnisec AG
	Organa
	Safeware
UK	Airtech Computer Security
	British Telecom
	Business Simulations

	Cambridge Electric Industries
	Codepoint Systems Ltd.
	Compserve Ltd. Compserve Ltd.
	Computer Associates
	Computer Security Ltd.
	Cylink Ltd.
	Data Innovation Ltd.
	DataSoft International Ltd.
	Datamedia Corporation, Ltd.
	Digital Crypto
	Dynatech Communcations Ltd.-(Northern office)
	Dynatech Communication Ltd.
	EngRus
	Fulcrum Communications
	GEC-Marconi Secure Systems
	Gelosia
	Global CIS Ltd.
	Gretag Ltd.
	Honeywell
	IT Security International
	ITV
	Incaa UK
	Interconnections
	International Data Security
	International Software Management
	J.R.Ward Computers Ltd.
	JPY Associates
	Jaguar Communications Ltd.
	Janus Sovereign
	Loadplan
	Logica
UK	Marconi
	Microft Technology Inc.
	Micronyx UK Ltd.
	Micronyx UK Ltd.
	Network Systems
	News Datacom
	Northern Telecom Europe Limited
	PC Security Ltd.
	PPCP
	Paradyne European Headquarters
	Plessy Crypto
	Plus 5 Engineering Ltd.

	Prosoft Ltd.
	Protection Systems Ltd.
	Racal
	Racal Milgo
	Radius
	S&S International
	Shareware plc
	Sington Associates
	Smart Diskette UK
	Smith's Associates
	Softdiskette
	Sophos Ltd.
	Stralfors Data
	Sygnus Data Communications
	The Software Forge Ltd.
	Time & Data Systems
	Tricom
	University College London
	Widney Ash
	Zergo
	Zeta Communications Ltd.
USA	3COM Corp.
	ADT Security Systems
	AO Electronics
	AOS
	ASC Systems
	ASD Software Inc.
	ASP
	AST Research
	AT&T
	AT&T Bell Laboratories
	AT&T Datotek Inc.
	Access Data Recovery
	Advanced Computer Security Concepts
	Advanced Encryption Systems
	Advanced Information Systems
	Advanced Micro Devices, Inc. (AMD)
	Aladdin Software Security
	American Computer Security
	Anagram Laboratories
USA	Applied Software Inc.
	Arkansas Systems, Inc.

Ashton Tate
BCC
BLOC Development Corporation
Banyan
Bi-Hex Co.
Borland
Braintree Technology
Burroughs
CE Infosys of America, Inc.
Casady and Greene
Centel Federal Systems Inc.
Central Point Software
Certus International
Cettlan Corp.
Chase Manhattan Bank, N.A.
Clarion
Codex Corp.
Collins Telecommunications Products Division
Command SW Systems
Commcrypt
Communication Devices Inc.
Complan
Computer Associates International, Inc.
Contemporary Cybernetics
Cryptall
Cryptech
Cryptex/Gretag Ltd.
Cylink Corp.
Cypher Comms Technology
DSC Communications
DataEase International
Datakey Inc.
Datamedia Corporation
Datamedia Corp. (DC Area)
Datawatch, Triangle Software Division
Datotek, Inc.
Dell Computer
Digital Delivery, Inc.
Digital Enterprises Inc.
Digital Equipment Corporation (DEC)
Digital Pathways
Docutel/Olivetti Corp.
Dolphin Software

	Dowty Network Systems
	ELIASHIM Microcomputers Inc.
	EMUCOM
	Enigma Logic, Inc.
	Enterprise Solutions Ltd.
	Fairchild Seminconductor
	Fifth Generation Systems, Inc.
	Fischer International
	Front Line Software
	GN Telematic Inc.
	GTE Sylvania
	Gemplus Card International
	General Electric Company
	Glenco Engineering
	HYDELCO, Inc.
	Hawk Technologies Inc.
USA	Hawkeye Grafix, Inc.
	Hilgraeve, Inc.
	Hughes Aircraft Company
	Hughes Data Systems Inc.
	Hughes Network Systems - California
	Hughes Network Systems - Maryland
	Hybrid Communications
	INFOSAFE
	Incaa Inc.
	Info Resource Engineering
	Info Security Systems
	Information Conversion Sevices
	Information Security Associates, Inc.
	Information Security Corp.
	Innovative Communications Technologies, Inc.
	Intel
	International Business Machines (IBM)
	Inter-Tech Corp.
	Isolation Systems, Inc.
	Isolation Systems, Inc.
	John E. Holt and Associates
	Jones Futurex, Inc.
	Kensington Microware Ltd.
	Kent Marsh Ltd.
	Key Concepts
	Kinetic Corp.
	LUCENT

Lassen Software, Inc.
Lattice Inc.
Lexicon, ICOT Corporation
Litronic Industries (Information Systems Division)
Litronic Industries (Virginia)
Lotus
MCTel
Maedae Enterprises
Magna
Mark Riordan
Massachusetts Institute of Technology
Matsushita Electronic Components Co.
Mergent International
Micanopy MicroSystems Inc.
Micro Card Technologies, Inc.
Micro Security Systems Inc.
MicroFrame Inc.
Microcom Inc. (Utilities Product Group)
MicroLink Technologies Inc.
Micronyx
Microrim
Microsoft
Mika, L.P.
Mike Ingle
Morning Star Technologies
Morse Security Group, Inc.
Motorola
NEC Technologies
National Semiconductor
Network-1, Inc.
Networking Dynamics Corp.
Nixdorf Computer Corporation
Northern Telecom Inc.
Norton
Novell
OnLine SW International
Ontrak Computer Systems Inc.
Optimum Electronics, Inc.
USA Otocom Systems Inc.
PC Access Control Inc.
PC Dynamics Inc.
PC Guardian
PC Plus Inc.

Paradyne Caribbean, Inc.
Paradyne Corporation
Paralon Technologies
Personal Computer Card Corp.
Pinon Engineering, Inc.
Prime Factors
RSA Data Security, Inc.
RSA Laboratories
Racal Datacom
Racal-Guardata
Racal-Milgo USA
Rainbow Technology
Raxco
Rothenbuhler Engineering
S Squared Electronics
SCO
SVC
Safetynet
Samna Corp
Scrambler Systems Corp.
Sector Technology
Secur-Data Systems, Inc.
Secura Technologies
Secure Systems Group Internationl, Inc.
Security Dynamics
Security Microsystems Inc.
Semaphore Communications
Sentry Systems, Inc.
Silver Oak Systems
SmartDisk Security Corp.
Software Directions, Inc.
Solid Oak Software
SophCo, Inc.
Sota Miltope
Stellar Systems Inc.
Sterling Software Inc. (Dylakor Division)
Sterling Software Inc. (System SW Marketing Division)
SunSoft
Symantec
TRW, Electronic Product Ltd.
Techmar Computer Products, Inc.
Techmatics, Inc.

	Technical Communications Corp. (TCC)
	Telequip Corp.
	Terry Ritter
	Texas Instruments, Inc.
	The Exchange
	Thumbscan, Inc.
	Tracor Ultron
	Trigram Systems
	Tritron Sytems
	Trusted Information Systems, Inc.
	UNIVAC
USA	UTI-MACO Safeguard Systems
	UUNet Technologies, Inc.
	United Software Security
	Uptronics, Inc.
	VLSI Technology, Inc.
	Verdix Corp. (Secure Products Division)
	ViaCrypt
	Visionary Electronics
	Wang Laboratories
	Wells Fargo Security Products
	Western DataCom Co. Inc.
	Western Digital Corporation
	Westinghouse Electric Corp.
	WordPerfect
	XTree
	Xetron Corp.
	Yeargin Engineering
	Zenith Data Systems
	hDC
	usrESZ Software, Inc.
YUGOSLAVIA	Sophos Yu d.o.o.

Senator LEAHY. Now, let me ask you this. On this program, how difficult would it be to decrypt it?

Mr. WALKER. Well, we have the decryption program in there on your phone and it is doing the decryption. You mean how difficult would it be for someone else?

Senator LEAHY. Yes; let us say that it is somebody else.

Mr. WALKER. This is standard DES, which is 56 bits of key. As Ray Kammer said, DES has served us very well for 17 years. It would take—well, there was an estimate last summer at the crypto conference that if you built a special purpose device for $10 million—this was actually an engineering estimate of some detail—you could exhaustively check the key space of DES in 3.5 hours, and that is the fastest that anyone has ever regularly predicted that.

Senator LEAHY. But Clipper Chip would take a lot longer than that.

Mr. WALKER. Clipper is 80 bits, and it is 2 to the 56th versus 2 to the 80th and it is 16 million times harder to do Clipper, so Clipper is very strong. Of course, and I don't want to hammer this too hard, but the question of what we do if DES gets too weak—well, one thing to do is to back up essentially DES processes together—it is actually three of them—and you can double the key length. So you can go to 128 bits with DES with the algorithms and with the software that is already available.

Senator LEAHY. With this, if you were sending something to me, I have got to know the key.

Mr. WALKER. That is right.

Senator LEAHY. One, I have got to have the program, but then I have got to know which key to use.

Mr. WALKER. Yes; and if you were to use it as a telephone you would like to set it up like the—well, if you want key escrow, you can run it the same way that the exchange of the key happens with the Clipper. If you don't like key escrow, you can do it the way they did it in the P version, which doesn't have key escrow. We could have, in fact, set up that same key exchange process. We just didn't have the time to do it.

Senator LEAHY. Now, you have linked them by an independent line, but you could have done this over regular telephone lines, couldn't you?

Mr. WALKER. That is right, yes, sir.

Senator LEAHY. And if you wanted to talk to your employees in London from an office in Maryland, you could use the same computer program to scramble those kinds of conversations?

Mr. WALKER. Yes.

Senator LEAHY. And data transmission, also?

Mr. WALKER. Yes; we have an alternative to PGP called Privacy Enhanced Mail, which is essentially the same kind of functionality that was talked about in the Wall Street Journal the other day. Some folks in England want it, the Ministry of Defense, in fact, and we have not been able to sell it to them because of the export laws.

The specs for PEM are internationally available and so we actually hired a scientist in England to rewrite the code from scratch using DES and RSA that is already available in England, and we

have demonstrated that to the British Ministry of Defense. They can buy it in England. We can't sell them our stuff here, so we have essentially done a second implementation. The irony is that the British export laws are such that we may well be able to export to the U.S. the version that we built in England which, of course, we couldn't ever send back to them.

Senator LEAHY. Now, the administration has stated that the use of key escrow encryption is going to be voluntary even for Federal agencies, and that no alternative encryption system is going to be outlawed.

Mr. WALKER. Yes; that sounds very good.

Senator LEAHY. Then what is the concern? If that is so, why is there concern about Clipper Chip?

Mr. WALKER. If that is so and if the numbers that I have projected down here are also right, one shouldn't have a concern about it. One is not certain that that is going to remain so forever, though. I mean, I am fearful that they are going to realize in 4 or 5 years, you know, this just isn't working; we are still having a problem. Then they will change the rules and it won't be voluntary.

Senator LEAHY. Yes; you are saying if Clipper Chips are not accepted on a voluntary basis. Then what do you think they are going to say? Whether you have got Clipper or DES or Pretty Good Privacy, or whatever, you have got to have a key escrow feature?

Mr. WALKER. It is clear—and I want to be very clear. I sympathize greatly with the law enforcement and the national security interests in this, and I am not trying to make their lives harder in this. As I was talking to the admiral just before we started here, he said this all started back when Admiral Inman let DES out. Well, indeed, that is the case. DES got out of the bag in 1976 or 1977 and we are now seeing it available around the world.

Their job, unfortunately, is going to get much harder whether we impose key escrow or whether we continue to control export control or not. I don't want to make their job harder, but I don't think it is reasonable for them to sacrifice U.S. national economic interests in the interest of keeping something that is already out of the bag and is eventually going to make life very difficult for them anyway.

Senator LEAHY. Unless they require the key escrow feature with everything.

Mr. WALKER. Indeed; key escrow, though, as we have seen in these devices and in the Tessera cards that are part of the Capstone Program, requires that it be done in hardware. I am a member of the NIST Software Escrow Alternatives Committee, and we indeed have met bimonthly, not biweekly, and we are struggling with whether there is any alternative here.

To require key escrow that you can't defeat trivially, you have to do it in hardware, and the whole point of this demonstration and thousands of others like it is encryption is available in software. No one is going to want to put key escrow along with this if, in fact, they have to add hardware to this when they already have it without it. So making a law that says you have to have key escrow will be one of the most significant laws that no one pays attention to that we have had in a long time.

Senator LEAHY. We have had a few of those over the years.

Mr. WALKER. Indeed; I mean, it's Prohibition all over again. It is going to be fun.

Senator LEAHY. I am too young to remember; that was before my time anyway, but I remember some of the stories my father told me about that.

You talk about NIST. Mr. Kammer, when he was testifying, said that NIST is open to other approaches. One, do you feel it is? I mean, you are serving with that advisory committee. Secondly, are there alternatives to Clipper Chip that could serve the objectives of protecting the privacy of communications, but not irreparably damage some of our national security and law enforcement needs?

I should emphasize in this that I am convinced both from open hearings and classified hearings that we have some very, very serious law enforcement needs and we have some very, very serious national security needs.

Mr. WALKER. I agree.

Senator LEAHY. In the national security area, I don't worry so much, as I have said on many occasions, about an army marching against us or a navy sailing against us, or an air force, because we are far too powerful for that. I am far more worried about a well-organized, well-directed, well-motivated terrorist group coming from abroad, one that could cause enormous physical damage as well as psychological damage. One that, I don't think it would be stretching it too far to say, could cause real damage to our constitutional liberties and our constitutional way of doing things, more so than the armies of World War I and World War II. Such a group could suddenly make us question everything from our search and seizure laws to our freedom of speech laws. That, as an American and one who has seen the importance of those constitutional safeguards, bothers me very much.

So do you see such alternatives?

Mr. WALKER. Well, there are alternatives that people have talked about. Sylvia McCauley at MIT has proposed for some time, and indeed apparently has some patents on some key escrow technologies. Basically, those end up being voluntary unless you can—I mean, easy to bypass is what I mean, making them—the law enforcement people can't insist that this is, in fact, going to be imposed everytime, and that seems to be a real hangup with the administration that if it is not something that can be imposed everytime it is used, then they are not interested in it. Unless we reorder the way in which we build our computers and our telephones, it is going to be very difficult, without something like the Clipper or the Capstone chip, to be able to have this happen everytime.

To your other point, I think this is why I have come to the conclusion after thinking about this for a year that we have a national dilemma here—the difference between individuals' rights to privacy and the law enforcement and national security needs. That is why I think it is so important that this be submitted for legislation and let all sides have their say and let the Congress decide whether we should impose this or not.

I really am not sure there is any other way to get out of this one. I mean, wiretaps are not an attractive thing to individuals, but we have decided that under certain circumstances wiretaps are OK.

We may well decide that key escrow is OK. It certainly does provide advantages if it becomes widely used, but I don't think—as the administration is now proceeding with this essentially on its own without any legislation, without any other use of the separation of powers of the Constitution, I don't think Americans are going to buy Clipper escrow devices, and so it is not going to achieve what they want.

If we considered legislation and as a country we decided this is the thing we need, for exactly the reasons that you were just giving, then fine. I will go along with it. I don't actually have that big a problem if our government is using—I mean, what I am suggesting is we put the key escrow center in the judiciary so that nobody in the executive branch supposedly can twist their arms.

We are in a situation where we have to trust our government for a certain amount of things. We shouldn't have to trust it for any more than we have to, and everytime we do something like this we should use all the separation of powers that we can. Put the enforcement in the executive branch, put the decisionmaking about the keys in the judicial branch, and keep them separate. It is the best system we have got and we should be using it.

Senator LEAHY. Mr. Diffie, how do you feel about this?

Mr. DIFFIE. Well, as I said, my first response to this is to look broadly at the technical resources of law enforcement and say, if you see the expanding possibilities not only of electronic surveillance but of DNA fingerprinting, of recognition of people in infrared photographs and a whole range of things that have become available to law enforcement as investigative and enforcement tools, it seems very clear that the failures of law enforcement in contemporary society are not failures of their technical capabilities.

On the other hand, the introduction of new technologies into society brings up the problem of how we embody existing traditions, values, procedures, et cetera, in using those technologies, and I think that is a thoroughly legitimate question about the way in which cryptography will be deployed. In talking about the intrinsic character of key escrow in storage cryptography, I was citing one example of that kind of thing.

Senator LEAHY. But you don't question, do you, the fact that there can be some very, very legitimate national security interests in knowing, for example, what kinds of communications might be sent from a country hostile to us or known to harbor and protect terrorists to people here in the United States, and that in protecting our national security there may be a very real need to know what was in that communication on a realtime basis?

Mr. DIFFIE. I don't doubt the value of communications intelligence. When you are talking about explicitly communications of terrorist groups that are foreign state-supported, I see no reason that the foreign state should be any more hesitant to supply them with COMSEC equipment than they are to supply them with AK–47's.

Senator LEAHY. You think that what they would do is give them the kind of communication equipment that we might not be able to decipher anyway?

Mr. DIFFIE. Well, you know, there has been a lot of pessimism in amateur circles over many years about communications intel-

ligence. The fact is that communications are quite hard to protect, and one of the important things about the sort of devices like the PSD 3600 is that they protect some aspects of your communications, but they don't do anything to protect the traffic analysis, the trap and trace, the pen registers, and all of that. So I think that you really have to take a comprehensive view of the communications intelligence and investigative techniques when you ask what the impact of cryptography applied at one level or another is going to be.

Senator LEAHY. Do you see the need for the ability to find out what somebody is saying, on a realtime basis for law enforcement inside our country? Consider a criminal holding somebody hostage for a ransom and threatening that if the ransom is not paid by a certain time, the person is going to be killed. We want to know where the communications are going, to try and determine where that person might be, with the possibility of a rescue prior to the person being killed. I mean, this is not a fanciful movie-of-the-week but could be a real-life situations.

Mr. DIFFIE. That is a very good example when you are talking about trying to trace calls, finding out where people are, and so forth. That is something which modern communications technology has made an overwhelming improvement in. If you look at the conventional wiretap, it is not so vastly much better than putting a bug in somebody's room. It is placed on what is called the local loop and it gives you access to the communications on the local loop with very little, if any, information about where calls are coming from.

If you look at modern communications intercepts inside digitized telephone systems, you are getting realtime information about where calls came from even if they are long distance.

Senator LEAHY. But you might not know what the call is if you don't know who is on there.

Mr. DIFFIE. I don't doubt that it is possible to construct a particular scenario that emphasizes any individual investigative technique. What I am trying to point out here is that the overall growth in investigative capability that has flowed from the changes in telecommunications gives law enforcement a wide range of new things that they can do that they couldn't do in the past, and that for them to accept those gleefully and then try to turn to any individual element with which they are now having more trouble without taking account of the fact that that is made up for by other resources is to give an unfair impression of the relative importance of particular investigative techniques versus very serious privacy concerns for business and individuals.

Senator LEAHY. Mr. Walker, what happens on the global electronic superhighway if Clipper Chip becomes the U.S. standard for encryption but other countries don't want to let it in?

Mr. WALKER. We will have a U.S. superhighway and we won't be part of what is happening elsewhere. If I might add just a minute to the comments that Whit was saying, yes, there is the possibility that some vital event will happen which we may lose to encrypted communications, but I think we have to balance that on the other side.

I participated 2 years ago in hearings with Congressman Brooks on foreign industrial espionage and, essentially, U.S. business is wide-open en masse right now to communications intercepts anywhere in the world, and we do not have cryptography available on our laptops as part of Microsoft's products or Novell's products or WordPerfect's products because we can't export it from this country. We don't have it ourselves either. You don't have it routinely available and neither do I.

So, yes, there is a concern that some event, a World Trade Center bombing, or whatever, may occur and we may lose something with that, but we are at grave risk that all of our technology that we are passing over the United States or global superhighway is wide-open at this time, and sometime we have to find a balance between the possibility of an event like a World Center Trade bombing employing cryptography and the absolute certainty that all of our industrial information is passing in the clear around the world, easy for our adversaries, governments and other countries, to pick off and listen to.

We have got to find a balance between those, and the balance has just swayed so far in favor of national security and law enforcement that it is going to eventually result in making the U.S. a third-rate power before we realize how significant that is.

Senator LEAHY. Larry?

Senator PRESSLER. Well, thank you very much, Mr. Chairman.

You may have covered this already, and if you have I apologize. I have been dealing with other committees this morning. As you are aware, critics of the administration's proposal argue that, as a practical matter, no criminal or foreign spy or terrorist of any sophistication would be foolish enough to us an encryption device designed by the NSA and approved by the FBI.

Why do we feel that people whose telecommunications the NSA and FBI want most to decode will be the very people most likely to use this technology?

Mr. WALKER. I suspect you should have been here during the previous people testifying. We agree with you.

Senator LEAHY. We spent about 2 hours going through that one.

Senator PRESSLER. OK.

Mr. WALKER. We don't disagree with the assertion that—well, I will say specifically this is an AT&T 3600 that does not use key escrow. It is currently for sale. There is a Clipper version that is also for sale. I think people who have any sense that they may be wiretapped are going to go to their AT&T store and buy this one rather than the Clipper one, for exactly the reason you mentioned.

Senator PRESSLER. Well, are there sufficient safeguards in the escrow system? You would have to have a court-authorized wiretap, and I guess two agencies would have to be involved. It sounds to me as though there are some fairly extensive safeguards built in.

Mr. WALKER. My personal opinion is with law enforcement operating within the law, the procedures that they are establishing—I have been briefed on this several times on the Computer System Advisory Board and other things—are going to be sufficient for this, law enforcement operating within the law.

I am concerned that law enforcement operating outside of the law doing something that is not authorized—these procedures may

not be good enough for that. I am not sure that you could ever have procedures that are good enough for that, which is the concern about establishing key escrow as a mechanism anyway, in any case, and why I believe we need to have legislation to review whether we really want this or not.

Mr. DIFFIE. I think my understanding is that in the early 1940's when Japanese Americans were interned, the information that was used to identify them was, in part, census information that was very explicitly legally—clear legal impropriety in using the census information for this purpose.

I think when we think about creating what the escrow system might become—that is, a repository of keys that could be used to read a vast amount of American traffic—we are considering creating a vulnerability, a very long-term vulnerability in the U.S. Communications System. In these discussions, it is always important to emphasize that as valuable as telecommunications are to us at present, they will be more valuable in the future. They will be more the essence of our society in a few years than they are now.

So I am very worried that we are creating something that is a fundamental danger to the security of our communications system under the guise of an improvement to the security of our communications system.

Senator PRESSLER. Now, Mr. Walker, you describe how present U.S. laws prohibit the export by your company of encryption products. Are you in favor of eliminating those laws completely? If not, what should be exported and what should be prohibited?

Mr. WALKER. I believe that there needs to be a balance found between super-good cryptography that is used by the U.S. Government to protect its classified information—I don't think that should be exported. What I am suggesting is things that are routinely available throughout the world ought to be able to be exported by the United States.

We have relaxed export controls on every kind of computer and telecommunications in the last couple of years except that involving cryptography. In the survey we are doing, which is done at a very low budget without a whole lot of fancy people working on it, we have found a very large number of DES and better products that are available throughout world. Why is it that U.S. companies are excluded from being able to participate in that?

So I am not suggesting that we ban export controls on cryptography as a whole. I am saying let us find what the level is that is available routinely around the world and establish that as the basis where U.S. companies can participate. If U.S. companies can participate in exporting things like DES, then you will find Microsoft and Novell and WordPerfect including encryption in their products so that when you want to protect a file from someone else reading it or when some company wants to use this to protect their very sensitive information, they will have the tools available to do it.

We do not have control in this country of the internal use of cryptography, but the use of export control has been so strong that it has, in effect, created a control of its use within the United States. It is legal to use DES to encrypt your Microsoft files, but you won't find a product that lets you do that relatively easily because the

people who build those products can't sell it to half the market that they have.

So we are in a situation which requires some degree of sense applied to it. Don't ban the export of cryptography in general. Good systems, military use systems, should not be exportable, but routine things that are available in the bookstores in London and in Germany and in Australia and South Africa—we ought to be able to sell those, too. That is what I am seeking, and I believe that is what the Cantwell and the Murray bills, in fact, are seeking to do, and I strongly encourage that the House and the Senate pass those as quickly as possible.

Senator PRESSLER. Thank you very much.

Senator LEAHY. Thank you. We will take a 2-minute recess to allow the next panel to set up.

[Recess.]

Senator LEAHY. During the break, someone asked me the numbers, and I reversed the cost estimate. NIST has estimated that $14 million is the cost of setting up the Key Escrow System, and $16 million is the annual maintenance cost. I forgot who asked me the question, but I hope they are still in the room. I wanted to correct it if I gave it just the other way around.

Admiral McConnell is the Director of the NSA, the National Security Agency, and has been for a couple of years. Before that, he served as head of the Intelligence Department of the Committee of the Chiefs of Staff of the U.S. Armed Forces. The admiral has been most patient in listening. By the end of this day, he and I will probably have heard more than either one of us ever wanted to hear on this subject.

Admiral I appreciate your being here because your involvement is absolutely essential in getting any resolution on this. I might note for the record that I appreciate the amount of time you have spent personally with me on this, and that the time your staff has spent. It has been very, very helpful, and I must say in my experience in 20 years in dealing with those in the intelligence agencies, I have never had anybody be more cooperative or more forthcoming than you have and I just wanted to publicly commend you on that, especially since some of the things that you are cooperative about I can't publicly thank you for, but I thank you in general.

Go ahead.

STATEMENT OF ADMIRAL J.M. McCONNELL

Admiral MCCONNELL. Mr. Chairman, I appreciate the opportunity to comment. As you know, I have submitted a statement for the record, but in the interests of time I would like to just make a few brief comments.

I noted that you started earlier this morning—it seems like hours and hours ago now——

Senator LEAHY. It was.

Admiral MCCONNELL. About the CNN/Time poll; 80 percent of Americans were against this. Just for interest, I pursued that a bit to read the question that was asked. Although the question wasn't published, it was stated in a way with pejoratives three times along the way to basically come down to, do you want the government reading your communications, as opposed to stating it in a

way to say this is not an enhanced or additional authority for the government to do its law enforcement mission, which includes legally authorized wiretaps. So I think the question was probably a little bit biased in the way it was asked.

Sir, your letter asked me to address what was NSA's role in this whole process, and it can be summed up very succinctly. We were the technical adviser to NIST that you heard from earlier and to the FBI and the Department of Justice. The FBI, in the legislation that they have submitted, recognized that they had a problem with the communications process going from analog to digital, referred to popularly as the digital telephony legislation. In conjunction with that, they began to appreciate the potential impact of encryption.

They came to us, as did NIST, in our role as directed under the Computer Security Act of 1987, and asked for technical assistance. Quite frankly, this was a very tough technical challenge for us. We sat down to sort through potential technical solutions and what we came up with was escrowed key.

Now, I would like to make the point that you only have three choices if you are going to encrypt something. You can use encryption that is exploitable, meaning that it is neither, not of sufficient key length or there is a weakness or there is something that would allow an adversary to break into it. You can use encryption that is exploitable, or you can use encryption that is unexploitable but uses an escrowed key. In my opinion, that is where we came out. We made encryption that is not exploitable. We factored in the escrow key, for all the reasons that have been enumerated for you this morning.

NSA has been castigated regularly in the literature on this subject as being the perpetrator and having sinister motives, and so on, and I would just like to take a moment here in public to try to put a little balance on some of those comments.

First of all, NSA has no domestic surveillance function. NSA has no law enforcement function. We do not target Americans. We have no direct association with law enforcement other than if we collect something in our mission of foreign intelligence that would be of use to law enforcement, we make that information available, just like we would make it available to any other agency of government or to the Congress.

The second point I would make is we certainly are a nation of laws. Our activities are governed by law and we have very extensive oversight not only in the executive branch, but also in the Congress, two committees, and you, of course, served on one of those committees. That oversight, sir, as you well know, is quite extensive on what we do.

Our mission is to target foreign activities, so anything that NSA is engaged in is strictly in a foreign context. Now, what are those things? Military capabilities; proliferation of weapons of mass destruction, even the creation of weapons of mass destruction; scientific and technical intelligence on weapons systems and ability of countermeasures to defeat U.S. systems; and, in fact, military operations, and you could extend it on to foreign government actions that would either harm their neighbors or would harm the inter-

ests of the country. All of those are very important things, and let me just use a current example.

Most who have focused at all on foreign relations are concerned about the events in North Korea. North Korea either has or they intend to build a nuclear weapon. They have a missile system that has a current range, we estimate, in the neighborhood of 1,000 km. They intend to build missiles with capabilities beyond 1,000 km. Now, that is of interest to the United States and it is of interest to our allies, the South Koreans, the Japanese, and others.

NSA's interest in this thing called cryptography and standards, and particularly international standards, is influenced by our service to the Nation to maintain awareness of what is going on in the world that impacts on not only military operations, but the formulation of foreign policy and that sort of thing.

Successful completion of our mission has saved lives not only in the military context, but in the civilian context, not only for the United States, but for our allies. We have provided information to our policymakers for the formulation of foreign policy. We did it last year, we did it last month, we did it yesterday, and we are doing it this morning.

Now, what I would like to do—since most of everything that I am involved with currently is classified and I am unable to speak freely on it, I want to try to give this a sense of relevance by speaking to a historical context.

In World War II in the Atlantic theater, the United States and Great Britain collaborated to break the communications of the enemy. Through the ability to read the communications of the enemy, we knew when they were planning battles, with what level force. We knew how to engage, when and where, and when it was to our advantage.

The U-boat force, the submarine force, was approaching success in shutting down the flow of war materials going from the United States to England and to Europe. The success in code-breaking allowed the United States to either circumvent the U-boats or to sink them. It made an incredible difference. Historians have credited, now that this information is public, World War II coming to completion in Europe, if not 2 years, at least 18 months, sooner than it would have otherwise.

Now, let me switch to the Pacific. The United States succeeded in breaking the code of the enemy in the Pacific. Because of that, with an inferior naval force, we immediately started to enjoy naval victory. The first was on the Coral Sea, the battle of the Coral Sea, and the second was at Midway. At the battle of Midway, the tide was turned.

Now, it is very interesting what happened in this historical context. The Coral Sea and the battle of Midway occurred in 1942. In the summer of 1942, a newspaper reporter became aware that the United States was breaking the communications of the enemy and it was published in a U.S. newspaper. It became a cause celebre and was repeated a number of times, and by the late summer the enemy had changed their communications process.

Coincident with that, the campaign in the Solomon Islands was initiated. It was long and it was bloody. We could not see their intentions. We did not understand what they were planning to do.

Therefore, it cost countless thousands of lives that, in my view, could have been avoided if our capability to exploit had been preserved.

NSA is involved in this level of activity every day, but as you well know, it is classified. If I spoke about it in public, what success we do enjoy today would disappear. So I use this historical context to try to provide some weight to what it means to the Nation.

I just would terminate on that particular subject in a current context by just advising you that the Secretary of Defense and General Powell at the conclusion of Desert Storm came out to NSA to personally thank the employees, the men and women, of NSA for the contributions that they made.

Sir, when we were asked to provide a technical solution, if there was a technical solution to this seemingly intractable problem, we started with a list of objectives, and I want to give those objectives. First and foremost, we just made ourselves a list of, as citizens, how would we like a technical solution to come out.

The first was, contrary to what appears in the popular literature, enhancement and protection of the privacy of Americans. That was number one on our list. The second was to protect public and private corporate information, business information; to promote U.S. competitiveness.; and, of course, the last objective was what we were asked to provide some thought to by Justice and NIST, and that was to allow law enforcement to monitor criminals or terrorists.

We conceived Clipper. It has been referred to here most often as Clipper. It is actually an algorithm and the name of it is Skipjack. Clipper is just one application of Skipjack. There are others. As has been stated earlier, it is 16 million times stronger than the current Federal standard, which is referred to as DES, or the Data Encryption Standard.

The idea was to escrow the key, hold it in such a way that it could be drawn for legitimate purposes. But if you really think about it for a moment, the auditability of the process and the accountability of the process improves the privacy of Americans over where it is today. Today, a political opponent, a used car salesman, a credit research bureau, a rogue cop, could intercept someone's communications. If they were using the devices that we have discussed here this morning with escrowed key, then the only way that you could break that communication would be with some oversight provided by a court in a process that is more accountable than what exists currently.

So I think, in my view, we have struck the proper balance between privacy protection and law enforcement access. I really believe when I have thought this through, and I have been working at it and thinking about it now for some 2 years, that the privacy of Americans is enhanced, not degraded. It not only is court-authorized, but we tried to make it analogous to the way we do nuclear weapons—two-agency control and two-man control, never allowing one person to have absolute control of the process. The existing wiretap authorities have not been expanded, and existing legal protections, in fact, in my view, have been strengthened.

NSA's INFOSEC mission, our mission which is not well known to most of those who talk about us and most discussions about what we do against foreign interests in terms of intelligence collection—we do have another mission, and that is information security for the government. We make the government's code, and because we are probably the most robust encryption activity available to the country, our expertise is drawn upon so we can take some of that technology that we have, in fact, spent millions of dollars on to make it available to resolve some of these other problems.

The administration did not take this lightly. They spent some 9 months reviewing it. They solicited and considered industry views. They concluded at the end of that deliberation that export controls on cryptography should be maintained as being in the best interests of the Nation so that it would not damage NSA's mission and our global responsibilities.

A number of reforms were announcing mandating speeding-up of the process and easing the regulatory burden to get, in fact, approved export items of a cryptographic nature exported—key escrow products that can be licensed quickly for movement out of the country so long as it is consistent with national security.

Now, a number of laws have been discussed today, and issues discussed today, and I think our two previous speakers captured it very eloquently. What I heard was one discussion of privacy and another discussion of profit motive or being motivated to do this because it may have some impact on U.S. business.

I would just highlight that there are other rules and regulations that people find offensive in the privacy sense, but to come into this hearing today I was electronically searched. To get on an airplane, I am electronically searched. The Congress has decided that that invasion of privacy is worth it in the interests of public safety. The same argument is being made with regard to court-authorized intercept of terrorist or criminal communications. Some would claim that these and other laws invade privacy. In my view, it is a balance of that privacy.

Key escrow is a technical solution to a very complex set of equities. As a matter of fact, at NSA that is how we refer to this issue. In addition to being a headache, we call it our equities issue. Whose equities are involved? I go back to what our original objectives were—Americans' privacy, corporate interest, law enforcement, and the competitiveness of U.S. business. So when we weigh all those equities, at least in my view, and I would say fortunately in the view of the administration which reviewed this, to include very active participation by the Vice President—he came down on the side of the most equities are represented and protected by the key escrow initiative.

So, that concludes my statement. I would be happy to try to answer your questions.

Senator LEAHY. Thank you; skipjack is for voice encryption now. Are you working on something even faster for data encryption?

Admiral MCCONNELL. Yes, sir. Currently, Skipjack can be made fast enough to keep up with any current or anticipated application, but there will be a need to go faster and we will either have to make Skipjack go faster or have a new approach. One of the things I might mention is, working for Defense—Defense had asked us to

come up with a technical solution for a way to use the information superhighway to exchange E-mail communications with business, with contractors, and so on, in a way that would be protected. That was why Skipjack was invented. The application is something we call Capstone. It is a PC card that just plugs in and provides you a lot of the functionality that has been discussed earlier.

When the FBI and Justice presented us with this other problem, we just took the Skipjack algorithm and applied it to basically a voice-only problem. Now, so far in the administration's review, the only thing that they have authorized in this FIPS, or this standard which is published by NIST, is for the voice and a low data rate application only. Where we are proceeding with Capstone, or this application for the Defense Department, that is strictly for government use, and whether it is going to be made available to the public and become a voluntary standard, and so on, is yet to be determined.

Senator LEAHY. I think your discussion of the Pacific battles was illustrative. Without going into any specific case, the hypothetical I used earlier today about threats from terrorist organizations—would you say that is a realistic hypothetical?

Admiral MCCONNELL. Sir, I thought Mr. Walker made a compelling argument for what is out there, and I just would highlight—and this is difficult for me to answer because it gets into sources and methods.

Senator LEAHY. Well, maybe I should ask it this way. Is it your estimation as one who deals with the security of this country that the United States, like most other Western nations, is not immune from terrorist threats from abroad?

Admiral MCCONNELL. No, no, sir, not at all.

Senator LEAHY. That is basically my question.

Admiral MCCONNELL. Not at all.

Senator LEAHY. Do you know whether foreign governments would be interested in importing key escrow encryption products to which they, not the U.S. Government, hold the keys?

Admiral MCCONNELL. Sir, this is a very interesting question and, in my view, when we have entered into discussions with our counterparts—we have counterpart relationships, as you are aware, and I would say that we in this country are probably a little further along in the decision process than some of our allies.

You used an example earlier, if you wanted to import cryptography into France, and I found it very interesting that you used France as your example because you can't import cryptography into France. When we have talked to our business partners, those that we deal with in the private sector, we frequently are asked, why can't you get my products into France? Well, the French pass laws that say you can't do that. They are going through this deliberation in the EC and in Europe and in the individual countries of Europe to determine how they are going to address this problem.

I just would use a phrase that I used when we had an opportunity to meet with the Vice President and discuss this issue and when we were coming to closure for decision. I said, sir, if you listen to the argument that unexploitable encryption should be available in this country to be exported anywhere we want to export it in the world, then you take the problem that we are attempting to

solve in this country and make it our allies' problem. Our allies have problems with criminals and drug dealers and terrorists. Are they likely to allow U.S. firms to import cryptography into their country that would shut out their law enforcement abilities? So these questions are very difficult. They are incredibly complex, and we are going through that process. I don't know exactly how it will come out.

Senator LEAHY. Have we had governments that have asked us, if we go forward with this, to work out a deal to share keys with them?

Admiral MCCONNELL. There are discussions with my counterparts and there are discussions at the law enforcement level. How it will turn out I can't forecast, but I would say that the objective of some of the various participants in the discussion is, if there is a law enforcement problem involving a foreign country and this technology is used, to work out some process that could help contribute to solving that law enforcement problem.

One of the things I worry about is this is exportable by an American by his own use. Now, he may not be permitted to use it in some given country because of the laws of that country, but he will be able to use it in other places. What I worry about is how do I ensure the privacy of that American who is in a foreign country. So these are very difficult questions that we will have to work our way through.

Senator LEAHY. But then we could have the possibility of these keys being in countries other than our own.

Admiral MCCONNELL. Yes, sir, we could.

Senator LEAHY. How does a country like France address the question that if they prohibit encryption devices or encryption programs that they may be just closed out of the whole information superhighway entirely?

Admiral MCCONNELL. Currently, the information superhighway is not encrypted, and that is what——

Senator LEAHY. But I mean if somebody used Pretty Good Privacy, for example, on there, it is encrypted.

Admiral MCCONNELL. Yes, sir.

Senator LEAHY. I mean, if you have got somebody sitting on the outskirts of Paris who clicks on to the Internet and if he uses Pretty Good Privacy to encrypt his message and send it to somebody in San Diego, CA, it is there.

Admiral MCCONNELL. Yes, sir. The laws, as they have been explained to me, in France are that you cannot import, export or domestically produce encryption without government approval.

Senator LEAHY. So, that person would be in violation of the law?

Admiral MCCONNELL. That person would be in violation of French law in that specific instance. Now, cases are made that this technology is available around the world, it is on Internet, it flows, and so on.

Senator LEAHY. Especially with the EC and worldwide trade, you can have companies who have got a branch in France and Italy, Ireland, the United States, Canada, Mexico, and Argentina. They may be constantly sending material back and forth, everything from E-mail to specs and diagrams and blueprints, and want to

encrypt it all. Doesn't a country like France get into an impossible situation if they are suddenly cut out of that loop?

Admiral MCCONNELL. Yes, sir, you can make that argument. So far, it hasn't gotten to that point. My choice, of course, would be if it is possible for key escrow standards to be established in a way that we can work it out with our allies, and so on, and that protects each person's equities. We don't really know where this is going.

I want to address the point that was made earlier by one of the preceding witnesses about the availability of these products. Sir, I don't deny that you can put something on Internet and it will flow, but I do a market survey of the globe every day, 24 hours a day, and what I can report back to you is, as a practical matter, for the kinds of things that are interested in from a foreign intelligence aspect there is not widespread use of some of these things.

Does that mean that there will not be widespread use in the future? We are judging human behavior, so we don't know exactly how that is going to turn out, but of the products that have been available to us to examine, they are not all as they have been advertised to be. Now, that is a cute way of saying the real answer is classified and I will discuss it with you at a later time. The arguments being made in public I have difficulty refuting because what I know is at a classified level.

Senator LEAHY. Well, we are going to go shortly into that part of the hearing, but let me ask you this. What if the key escrow encryption chip—say, the Clipper Chip—is not widely accepted on a voluntary basis? Now, I understand some of the things that are being done to make it more acceptable, such as the government buying and the cost going down, and so on and so forth. Would the intelligence and law enforcement agencies recommend that all encryption systems—DES, Pretty Good Privacy, whatever else—have a key escrow feature, with the government holding a duplicate set of the keys?

Admiral MCCONNELL. On a mandatory basis?

Senator LEAHY. Yes.

Admiral MCCONNELL. That is not the intent of the administration.

Senator LEAHY. Well, would that suffice in order to allow exportation?

Admiral MCCONNELL. Currently, there are products exported from the country that do not have escrow key. As a matter of fact, the vast majority of those who desire export——

Senator LEAHY. They are not as good either.

Admiral MCCONNELL. No, sir. That is correct. Skipjack is no trivial algorithm. I mean, if you were to attack this—as it has been described earlier, as you run something to exhaustion and if it is robust—if you were to attack it, I mean you are into not hundreds, but thousands of years before you could ever run it to exhaustion.

Senator LEAHY. Well, let us think of it another way. Suppose you have got a Clipper Chip the Key Escrow System and everything else, and somebody double encrypts it, say, using DES. Can you tell from looking at the cipher, the encrypted text, whether the underlying message was encrypted?

Admiral MCCONNELL. It would be difficult. If one were to use——

Senator LEAHY. In other words, I am asking you if double encrypting can defeat Clipper Chip.

Admiral MCCONNELL. Yes, sir, it clearly could, but there would be no advantage to using Clipper and, let us say, DES, for example. You would just use DES. Assuming that you were a criminal and the government held the keys, getting through Clipper you would still have the same level of protection, which is a 56-bit key, a robust algorithm known as DES.

Senator LEAHY. Let me ask you about the family key. Every Clipper Chip has the same family key programmed into it, if I understand it correctly. It is used by law enforcement to decode an intercepted serial number or the identifier that is at the beginning of each encrypted conversation.

Now, if somebody got unauthorized access to the chip family key, can they do anything with that? For example, can they keep track of communications traffic back and forth between a particular chip?

Admiral MCCONNELL. They would be able to read the serial number on the chip.

Senator LEAHY. Is that about it?

Admiral MCCONNELL. Yes, sir, but that is kind of an interesting question, sir. With your law enforcement background, I am sure you are aware that if you are conducting a criminal investigation every phone call—records are kept by the phone company for tolling purposes, so if you are a criminal investigator with a case open, you just subpoena those records or get the records and they are made available to you. So there wouldn't be any advantage to—if I were law enforcement, I sure wouldn't want to break the law to do something I could get with due course.

Senator LEAHY. But they couldn't use it to in any way decode?

Admiral MCCONNELL. No, sir.

Senator LEAHY. They would still need the——

Admiral MCCONNELL. No, sir, and they wouldn't get any more information than they already get in current activity.

Senator LEAHY. Well, Admiral, unless you want to add something in open session, we will go over to the bubble.

Admiral MCCONNELL. No, sir. Thank you for the opportunity to comment.

Senator LEAHY. Thank you.

[The prepared statement of Admiral J.M. McConnell follows:]

PREPARED STATEMENT OF VICE ADMIRAL J.M. MCCONNELL

Good morning. I appreciate the opportunity to discuss with you NSA's interests in and involvement with the Administration's key escrow encryption program and its decision to encourage the use of the government designed encryption microcircuits, commonly referred to as CLIPPER chips. These microcircuits, or chips, provide robust encryption, but also enable law enforcement organizations, when lawfully authorized, to obtain the key that unlocks the encryption. The President's program advances two seemingly conflicted interests—preserving critical electronic surveillance capabilities, on the one hand, and providing excellent information systems security, on the other. I will discuss the role we played in support of this program. I will also discuss NSA's interests, both in general and in respect to the President's program.

NSA'S ROLE IN THE PRESIDENT'S INITIATIVE

Our role in support of this initiative can be summed up as "technical advisors" to the National Institute of Standards and Technology (NIST) and the FBI.

As the nation's signals intelligence (SIGINT) authority and cryptographic experts, NSA has long had a role to advise other government organizations on issues that relate to the conduct of electronic surveillance or matters affecting the security of communications systems. Our function in the latter category became more active with the passage of the Computer Security Act of 1987. The Act states that the National Bureau of Standards (now NIST) may, where appropriate, draw upon the technical advice and assistance of NSA. It also provides that NIST must draw upon computer system technical security guidelines developed by NSA to the extent that NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in federal computer systems. These statutory guidelines have formed the basis for NSA's involvement with the key escrow program.

Subsequent to the passage of the Computer Security Act, NIST and NSA formally executed a memorandum of understanding (MOU) that created a Technical Working Group to facilitate our interactions. The FBI, though not a signatory to the MOU, was a frequent participant in our meetings. The FBI realized that they had a domestic law enforcement problem—the use of certain technologies in communications and computer systems that can prevent effective use of court authorized wiretaps, a critical weapon in their fight against crime and criminals. In the ensuing discussions, the FBI and NIST sought our technical advice and expertise in cryptography to develop a technical means to allow for the proliferation of top quality encryption technology while affording law enforcement the capability to access encrypted communications under lawfully authorized conditions.

We undertook a research and development program with the intent of finding a means to meet NIST's and the FBI's concerns. The program led to the development of two microcircuits or chips. The first was an all-purpose chip with encryption, public key exchange, digital signature, and hashing functions. The second contained the encryption function only and is intended for use in devices in which digital signature and hashing are not needed and key exchange is provided by some means outside the chip.

Throughout the design and development of the key escrow encryption system, we placed an emphasis on providing for the protection of users' privacy. We focused on ways in which we could preserve law enforcement's existing capabilities without undermining privacy rights and protections embodied in current law.

One of the technical solutions to these privacy concerns is the split escrowed key. All chips have been designed to be programed with their own identification number and a unique key that could be used to unlock the encryption. Because the chip-unique keys can be used to unlock the encryption, we also devised a means to split the keys and to keep each part with a different custodian. Neither part is useful without the other. The parts of each chip's unique key are separately escrowed with two trusted custodians at the time the chip is programmed. In this way, when law enforcement officials conduct a court-authorized wiretap and encounter this encryption, they can identify the chip being used and obtain the corresponding chip-unique key from the custodians, again using the court authorization. This concept of splitting the key into two or more parts is a sound security technique which provides a safeguard against unlawful attempts to obtain keys and illegally access protected communications. This also provides security against the risk that a single custodian might lose control of the keys, making the corresponding chips vulnerable to decryption.

In addition to splitting the key, the system has been designed so that the chip-unique key components are encrypted. Neither the custodians nor law enforcement officials know even a portion of the unique keys. The unique keys are only decrypted in a special device used to decrypt communications encrypted with key escrow chips. These devices are, of course, kept under strict control to ensure they are used only in connection with authorized wiretaps.

With the key escrow concept, the U.S. is the only country, so far, proposing a technique that provides its citizens very good privacy protection and maintains the current ability of law enforcement agencies to fight crime. Other countries are using government licensing or other means to restrict the use of encryption. We have gone to great lengths to provide for both the privacy and law enforcement interests and I believe we have developed the best technical approach to date. As a result, I believe the key escrow encryption system actually enhances privacy protections when you consider that most people currently use no encryption. Widespread use of CLIPPER will make it easy for people to take advantage of the benefits that high quality encryption offers.

NSA'S INTERESTS IN THE KEY ESCROW INITIATIVE

While our role in this initiative has been that of technical advisor to NIST and the FBI, we are very interested in the outcome and its impact on NSA's two missions, information security and foreign signals intelligence.

NSA has a mission to devise security techniques for government communications and computer systems that process classified information or are involved in certain military or intelligence activities. In keeping with the Computer Security Act of 1987, we also make available to NIST the benefits of our security expertise so they can, as appropriate, use it to promulgate the security standards applicable to the systems under their purview, i.e. federal systems that process sensitive unclassified information. Through our support of NIST and the promulgation of standards for federal systems, we advance a goal we all share—assuring that Americans have available to them the products they need to secure their communications and computer systems.

The NSA Information Systems Security, or INFOSEC, organization is continuously striving to understand the threats to information systems and to devise new or improved methods to protect against those threats. While most of us only consider the security of our systems when there is a much publicized case of computer hacking or intercepted cellular calls, NSA's INFOSEC people recognize the threats are ever present. They possess a unique sensitivity to the nature and the extent of these threats, and these insights into information system vulnerabilities form the foundation for building information systems security products. We have applied this knowledge and unrivaled cryptographic expertise for over 40 years in designing security products for U.S. communications and information systems that I can say with confidence and pride, are second to none.

Key escrow technology advances NSA's INFOSEC interests. For one thing, the encryption microcircuits provide excellent security, better by far than the Data Encryption Standard (DES). We will use these chips in products to secure information systems for which we are responsible. We are also pleased to see such robust security available for the voluntary use of all Americans. To the extent that we can use commercial off-the-shelf products as a basis for securing information systems under our purview, the cost to all users will decline. Moreover, widespread use of these products will enhance the interoperability of systems among all users. All of this is to the good of our INFOSEC interests.

The key escrow initiative was designed to accommodate all of our interests in assuring the privacy of our communications and in preserving law enforcement access to communications when necessary and lawfully authorized. This accommodation reflects the Administrations realization of the importance of effectively managing this technology so as to preserve our electronic surveillance capabilities. Whether it is law enforcement's wiretap-derived evidence of a crime or intelligence information regarding a foreign government, we as a nation use the product of electronic surveillance to assure the national security and the public safety.

From a signals intelligence standpoint, we are only concerned with the use of encryption by targets of our foreign intelligence efforts. Clearly, the success of NSA's intelligence mission depends on our continued ability to collect and understand foreign communications. Encryption, a technique for scrambling communications so that unintended recipients cannot understand their contents, can disrupt our ability to produce foreign signals intelligence. Controls on encryption exports are important to maintaining our capabilities.

At the direction of the President in April, 1993, the Administration spent ten months carefully reviewing its encryption policies, with particular attention to those issues related to export controls on encryption products. The Administration consulted with many industry and private sector representatives and sought their opinions and suggestions on the entire encryption export control policy and process. As a result of this review, the Administration concluded that the current encryption export controls are in the best interest of the nation and must be maintained, but that some changes should be made in the export licensing process in order to maximize the exportability of encryption products and to reduce the regulatory burden on exporters. These changes will greatly ease the licensing process and allow exporters to more rapidly and easily export their products.

In addition, the Administration agreed at the urging of industry that key escrow encryption products would be exportable. Our announcement regarding the exportability of key escrow encryption products has caused some to assert that the Administration is permitting the export of key escrow products while controlling competing products in order to force manufacturers to adopt key escrow technology. These arguments are without foundation.

Many non-key escrow encryption products have long been licensed for export. Such products will continue to be approved for export notwithstanding the fact that key escrow encryption products are becoming available. Moreover, we will continue to review proposed exports of new encryption products and will license them for export in any case in which the export is consistent with national interests. Finally, as I mentioned earlier, the Administration is in the process of implementing reforms of the licensing process to speed licensing and reduce the licensing burdens on encryption exporters. These reforms will benefit exporters of key escrow and non-key-escrow encryption alike. In short, we are not using or intending to use export controls to force vendors to adopt key escrow technology.

CONCLUSION

In sum, I believe the President's initiative is a reasonable response to a very difficult set of issues. It accommodates users' interests in security and the law enforcement interest to unlock encryption when lawfully authorized. The procedures for escrowing key are being developed to ensure the security of the devices is not compromised by the escrow system. There are, to be sure, issues to be ironed out, but I am confident we will work out the wrinkles.

I would be pleased to answer any questions you may have.

Senator LEAHY. The subcommittee stands adjourned.

[Whereupon, at 12:41 p.m., the subcommittee was adjourned.]

APPENDIX

Additional Submissions for the Record

Prepared Statement of Computer and Business Equipment Manufacturers Association

SUMMARY

CBEMA represents the leading U.S. providers of information technology products and services.[1] Its members had combined sales of $270 billion in 1992, representing about 4.5% of our nation's gross national product. They employ more than 1 million people in the United States. CBEMA develops and advocates public policies beneficial to the information technology industry in the U.S., participates in all pertinent standards programs worldwide, and sponsors the U.S. committees developing voluntary standards, domestically and internationally, for information technology.

CBEMA initially reacted to the President's key escrow/Skipjack[2] initiative during hearings in June held by the Computer System Security and Privacy Advisory Board to the National Institute of Standards and Technology. The CBEMA statement voiced our industry's concerns about individual privacy, the marketability of products, both in the U.S. and abroad, the technical difficulties of incorporating key escrow/Skipjack into devices, and the cost/competitiveness problems associated with key escrow/Skipjack.

This paper further develops several of those issues and offers CBEMA's recommendations that will meet both law enforcement and private sector needs in the U.S. and abroad.[3] This document neither endorses nor criticizes the concept of key escrow. It does, however, examine the realities of a marketplace that has evolved without a key escrow system and concludes that:

- The negative implications of using key escrow/Skipjack for protecting typical information technology applications far outweigh the potential benefits.
- The Data Encryption Standard should be recertified.
- An encryption strategy should be developed in a public forum.
- Sponsored research is needed to develop a software embodiment for key escrow.
- Encryption export controls need revision.

INFORMATION TECHNOLOGY HAS BECOME GLOBAL AND NETWORKED

Each year the market for information technology equipment and related products becomes increasingly global. During the 1970s and early 80s the majority of sales by U.S. manufacturers was domestic. Today, however, between half and two-thirds of all sales by U.S. information technology manufacturers are to foreign customers.

[1] See appended list of members.

[2] "Key escrow" refers to the general concept; for specificity we have used the term "key escrow/Skipjack" to refer to the technical embodiment currently under discussion.

[3] The viewpoint in the paper is that of vendors in a global market seeking to meet their customers' needs, including those of the government. Therefore, its focus is on business and economic implications, and it expresses no positions on the social, political or legal issues surrounding the key escrow/Skipjack proposal.

The globalization of the market for information technology products has paralleled a revolution in information technology use that has fundamentally changed the then existing modes of operation. In the 1970s and early 80s most businesses implemented large main frame computer complexes that served employees at the site or remote terminals connected to a single computer system. Because few of these computer systems were connected with other computer systems, most security measures were directed at the computer site.

Today, however, interconnected computers are the norm. Digital networks—such as electronic mail systems, Internet, and digital telephone system—increasingly are relied upon for routine as well as sensitive communications, and security is required for those interconnections and for the personal computers being interconnected to those networks. Continuing rapid development of information technology products depends heavily upon wireless technology, and security will be required for communications among these products as well.

For the future we must develop processes that will support successful development of a National Information Infrastructure (which will in reality be global). In this development major concern is already focused on how to safeguard information on the network.

ENCRYPTION HAS BECOME A CRITICAL COMPONENT OF INFORMATION SECURITY

During the evolution of information processing, encryption also gained significance. Although some vendors implemented their own versions of encryption, the Data Encryption Standard (DES) and public key algorithms (such as RSA) became the leading cryptographic techniques. DES is an American National Standard as well as a Federal Information Processing Standard (FIPS). Today a large installed base of devices and systems rely on DES and RSA. The banking industry, for example, has its standards for interbank operations such as funds transfer based on the DES. Encryption based on the DES standard also is used increasingly in over-the-counter software products and as an element of larger hardware and software solutions.

In the 1980s customers demanded that vendors provide products which would operate with one another. A major response to this demand was creation of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Open Systems Interconnection (OSI) architecture, which provides security services including encryption among its specifications. In another response, some vendors formed the Open Software Foundation (OSF) to help standardize implementation of fundamental software tools across platforms such as the UNIX operating system. OSF has announced a set of network software products implementing the distributed computing environment (DCE) which uses the DES algorithm for purposes of authentication, data confidentiality and integrity, and network access control. The Internet Society utilizes both DES and RSA to provide its Privacy Enhanced Mail (PEM) facility. This technique is very close to that utilized in the X.400 messaging recommendation and supported by the ISO/IEC OSI Directory standard. The American National Standards Institute (ANSI) standards committee for banking, X9, has also recently adopted these techniques. In short, the infrastructure to support security services for business needs, e.g., electronic data interchange of transaction documents, health care automation and so on, is rapidly being deployed.

A key factor in the acceptance of DES and RSA is the confidence in their cryptographic strength and overall integrity that has developed over years of public scrutiny.

Demand for encryption is expected to increase more rapidly as techniques become more simplified. In the past, utilization of encryption was a deeply considered decision made by user management, since employing it imposed significant costs, especially those of key management. But simpler key management techniques have been developed that maintain a high level of security. One approach, for example, involves using a public key technique to deliver the DES key and DES to encrypt the contents for confidentiality. As an example of another approach, the DCE noted above generates session keys and manages the keys with total transparency to the user. A result of this simplification has been the rapid evolution to using encryption for applications in the commercial marketplace, because encryption services may be included in typical information technology applications at a much lower cost.

Whole new classes of application and product have been developed which incorporate encryption in the product design. One example is automated teller products. In such systems the customer is assured of security without having to think about how this is achieved. Other examples of this product-design-encryption trend are non-repudiation and digital signature services in electronic data interchange and privacy enhanced mail on the Internet These newest developments indicate that

encryption will become more, rather than less, prevalent in the future—both in organizationally controlled environments and in stranger-to-stranger operation.

DESIGN & INTEROPERABILITY CONSIDERATIONS REQUIRE FLEXIBLE ENCRYPTION, AVAILABLE IN BOTH HARDWARE AND SOFTWARE

The importance of computer security has dramatically increased due to widespread deployment of distributed processing, open network highways, and greater interoperation of computing platforms from many vendors. To beet this challenge, the computer industry requires consistent cryptographic standards for algorithms, procedures and applications. It also requires vendor access to information regarding algorithms for freedom of implementation in various technologies and products. This access and the resulting flexibility of implementation are largely responsible for the success of DES and public key encryption. As a result of this evolution interested vendors have negotiated licenses for the use of RSA. DES licenses are available royalty free.

Other design and cost issues emerge when the application of key escrow/Skipjack to wireless technologies is examined. Experience to date with cordless and cellular phones shows that their vulnerability to being overheard is a significant weakness. The cutting edge of information technology products, both personal and for the office, rely on wireless technology. Thus, many organizational customers will demand encryption capability to maintain the confidentiality required for their operations. The vendor's margins for these devices are expected to be slim, due to fierce competition and savvy, cost-conscious customers. Thus a premium will continue to exist for flexibility in implementation and low cost.

Current rules-of-thumb put the final price of a component at four times its cost to the manufacturer. Therefore the cost of key escrow/Skipjack (currently estimated at $25) and its support circuitry could significantly raise a product's price compared to the price of the same product without this encryption capability. It is apparent that a hardware encryption method such as key escrow/Skipjack is a costly alternative to software embedded encryption, even with royalties.

For portable and personal devices there will be an additional issue raised by the size and power requirements of the physical embodiment. The limiting performance factor for such devices is battery life. Key escrow/Skipjack, then, must be designed to cause a very low power drain. Combining this with the restricted physical space available, an attractive design approach would be to use software encryption, since the designers typically seek to minimize the number of chips in the device.

The requirements of hardware/software implementations and interoperability are two vital requirements that are not met by key escrow/Skipjack. In summary, the classified nature of the Skipjack algorithm creates the following problems for industry:

1. Selection of a new, classified, unpublished algorithm for domestic commercial usage is counter to the need for broad interoperability and management of cryptography that is required by the customer.
2. The choice of classified technology for commercial applications restricts the industry's ability to effectively and efficiently meet market needs. Since details are unknown to product developers, it is impossible to implement that capability by embedding it in systems products. With a single classified key escrow/Skipjack implementation, this function cannot be effective in a broad range of products requiring cryptographic capability. Whereas published algorithms have been effectively engineered into products that range from a smart card" to a mainframe, they do not rely on a single technological implementation.
3. Because the Skipjack algorithm is classified, software implementations are excluded. In some cases encryption, while needing to be secure, does not need to be fast. In this environment a software implementation might be the wisest, least expensive solution.
4. In certain applications there is a requirement to selectively apply encryption to data. For example, in supporting electronic mail the address on the "envelope" must be in the clear, even though the "letter" is encrypted. This will be difficult to implement without customizing the encryption service. Since Skipjack is classified and isolated on a chip, such customization is difficult at best.

THE CONDITIONS DO NOT EXIST FOR MANDATORY IMPLEMENTATION OF KEY ESCROW/ SKIPJACK

Implementation of key escrow/Skipjack as a standard for data in the U.S., through extensive government procurement, would increase costs to the Government

by the need to design security products for which there is very limited overseas demand. Specifically, the U.S. Government's guaranteed access to communications made with products that incorporate key escrow/Skipjack will make the products either unacceptable or highly undesirable for most non-U.S. customers. Other techniques (e.g., DES) will therefore continue to be used, even though they are subject to restrictive U.S. export controls. The resulting fragmentation of the market will provide an advantage to overseas producers, who will continue to market DES-based and other security products both in the U.S. and abroad.

The DES standard will continue to be used worldwide regardless of volume purchasing by the U.S. Government. The DES standard is already widely used in the banking industry, for commercial applications within the U.S., and by governments outside the U.S. Implementations are available in both hardware and software; investment in the installed base of DES applications is considerable. Consequently, U.S. firms will continue to be solicited to provide data encryption products based on DES. Some users stand to be disadvantaged commercially by implementation of key escrow/Skipjack. In the banking industry, for example, systems would have to be designed to this standard for communication with government agencies (e.g., the Federal Reserve); however, institutions will have to continue to maintain data communications based on both standards to serve non-U.S. financial institutions and institutions that do not communicate with the Federal Government.

Key escrow/Skipjack is not compatible with implementations worldwide. Since customers demand that devices interoperate with the installed base to protect the investment they have made in hardware, software and administration of their systems, they will be unlikely to accept devices implementing key escrow/Skipjack because they lack the interoperability they need.

INDEPENDENT OF KEY ESCROW/SKIPJACK, EXPORT CONTROLS ON ENCRYPTION SOFTWARE AND HARDWARE MUST BE RATIONALIZED

Although the Administration's key escrow/Skipjack proposal does not specifically state the export control policy to be applied to this technology, no discussion of encryption can omit the export control issue.

The U.S. controls all encryption products for export. Data encryption[4] is controlled as a military item by the Department of State. As a matter of policy, a virtual embargo is in place for all exports of products containing data encryption to commercial customers other than banks, even to end-users located in countries that are America's closest allies. This policy disregards the legitimate commercial need for strong encryption capability.

Despite the fact that many types of software products containing encryption, particularly those in the public domain and those that are sold on a mass-market basis, are beyond effective control, and also the fact that many overseas vendors are now offering strong encryption, the U.S. has made no significant change in its approach to controlling these products. As a result, U.S. companies experience a loss in potential sales and increased corporate security risk with no commensurate benefit in terms of national security.

Key escrow/Skipjack does not "cure" the fundamental problems of U.S. export controls on encryption. As the key escrow concept underlying the approach is designed to ensure access by the U.S. Government, products based on it will be either unacceptable or highly undesirable for most overseas customers-even in the absence of export controls. Thus export controls on this device are not needed or desirable.

In the study of export control issues, CBEMA and its members have received requests to provide the "facts" proving current controls impose a serious reduction in U.S. company competitiveness. Our consensus analysis of the issue for the future is contained in this paper. Our consensus comments about the past are in our statement for the June 2 MST hearings. Our members individually have agreed to make available company proprietary information under appropriate arrangements to ensure confidentiality.

CBEMA RECOMMENDATIONS

This paper has examined the design, interoperability, cost, potential customer acceptance and export control problems that are obstacles to the widespread use and acceptance of key escrow/Skipjack. Yet CBEMA members are well aware of the concerns of the U.S. government that led to the development of key escrow/Skipjack. In an attempt to balance those concerns with the realities of the marketplace,

[4] We use the term "data encryption" to include all forms of controlled encryption for confidentiality. This term includes "file encryption."

CBEMA offers the following recommendations regarding the key escrow/Skipjack proposal.

1. CBEMA members have had much discussion regarding the implications of key escrow/Skipjack to the future of the information and telecommunications industries. It is predicted that much of the previous separate technology of voice, fax and data will converge. Current and future multimedia personal workstations are examples of this convergence. In this environment the workstation will serve as a voice answering machine, take voice dictation, fax information from a fax modem and have the ability to store, manipulate and send images. Indeed, the confusion on the possible scope of key escrow/Skipjack was emphasized in the draft Federal Information Processing Standard (FIPS) regarding escrowed encryption (EES). This draft contained an unusual description of the scope by defining the word "data" as to include voice, fax, and computer information sent across telephone lines.

   Before the merger of these technologies, it was appropriate to look at each application and build hardware and software satisfying that specific application. Because of this former approach, there is limited imbedded investment within government and industry in telephone and telephony products used in encrypting unclassified voice communications. It would therefore seem that financial and operational dislocation problems would be minimized if the use of key escrow/Skipjack were restricted to these traditional applications and its use were to remain voluntary.

   However, employing key escrow/Skipjack even to secure traditional telephony applications can be expected to create undesirable product design and market ramifications for computer and software industries due to the previously mentioned convergence of these technologies. It seems inappropriate that the government would continue to view these as separate and distinct application areas when the rest of private industry is enjoying the benefits from an integrated approach. There is the possibility that key escrow/Skipjack could conceivably satisfy the need for encryption in government and commercial traditional telephony applications if the resulting devices could accommodate the space, cost, through put and power constraints that are imposed by the key escrow/Skipjack devices. Such investments should be made with the knowledge that successful completion of Recommendations two through four could obsolete that investment.
2. Key escrow/Skipjack, given present limitations, is unsuitable for applications in which there is an embedded base of DES or similar capability, particularly of the software variety. Therefore CBEMA recommends that DES be recertified as a federal standard for data communications for an additional five years. During these five years, government should collaborate with industry to achieve a mutually acceptable encryption standards strategy, applicable to all communications, i.e., voice and data, and narrow and broad band communications. Both DES and public key encryption should be considered in this effort, including the possible application of the concept of key escrow to these technologies.
3. Develop an encryption strategy in a public standards forum, i.e., the American National Standards Institute Accredited Standards Committee on Information Processing Systems, X3, in the U.S., and then the International Organization for Standardization/International Electrotechnical Commission Joint Committee on Information Technology, JTC–1, internationally, with the objective of achieving one or more encryption standards capable of meeting the requirements and acceptable to all users. CBEMA strongly recommends that all relevant issues, including international acceptance, be considered with the specific objective of agreeing on one or more international standards to satisfy the public need for encryption for information transfer of every kind in various environments.
4. The government has requested industry's assistance to develop a software embodiment of Key Escrow/Skipjack. The government should issue a request for proposal through an agency, e.g., the Advanced Research Projects Agency, for pursuit of a software implementation of a strong encryption facility to be accomplished without compromising the facility's nature.
5. In view of the widespread availability of encryption products worldwide and the legitimate commercial need for encryption products, CBEMA urges that the following improvements be made with regard to export controls on encryption. These improvements will more closely align the U.S. with COCOM policies and will also enable U.S. companies to compete internationally:

   - Software that is publicly available or mass market (per the internationally accepted COCOM definition) should be decontrolled except for shipment to terrorist and embargoed countries.

- Hardware implementations of decontrolled software should be similarly decontrolled.
- Dual-use encryption (not specifically designed for military applications) should be controlled under the Export Administration Act and be subject to Department of Commerce jurisdiction, not controlled under the ITAR.
- Encryption functionality currently under Commerce Department jurisdiction and controlled under national discretion procedures should be decontrolled.
- In view of the fact that overseas demand for key escrow/Skipjack will not pose any danger to the United States, encryption functionality provided by key escrow/Skipjack should not be controlled for export.

PREPARED STATEMENT OF THE UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

The U.S. Council for International Business is pleased to submit its views on encryption and Clipper.

Introduction

The U.S. Council represents American business positions in the major international economic institutions, and before the Executive and Legislative branches of the U.S. Government. As the U.S. member of the International Chamber of Commerce (ICC), the Business and Industry Advisory Committee (BIAC) to the OECD, and the International Organization of Employers (IOE), the U.S. Council is the American business group that officially consults with the key intergovernmental bodies influencing international business. Its primary objective is to promote an open system of world trade, finance, and investment.

The Need for an International Encryption Policy

The U.S. needs a comprehensive encryption policy that provides security for communications. Such an encryption policy should preserve the right of privacy for business and individuals in voice and digital communications transmissions. At the same time, we recognize the government's legitimate interest in accessing telephone communications for law enforcement and national security reasons. We therefore support the U.S. Administration's directive to Government agencies to develop a comprehensive encryption policy, as announced one year ago on April 16, 1993.

An encryption policy, however, is not solely a domestic issue. The presence of an internationally accepted encryption policy is essential, as companies operate in a global marketplace. International businesses are demanding seamless webs of communications networks whereby information can flow in a free and secure manner. Today secure communications are critical to intra- and inter-corporate communications and transactions, as hackers, criminals and unauthorized parties find increasingly sophisticated tools to violate the privacy and security of communications systems. Companies need effective, internationally accepted cryptographic standards for secure communications and digital signatures to conduct their operations. Although highly technical in nature, such standards could have a profound effect upon the competitiveness of U.S. manufacturers and users of products with encryption features.

"Clipper"

The Executive Branch's announcement in April 1993 of its encryption initiatives raised great concern among U.S. businesses. Since these initiatives (Clipper and Capstone) do not employ internationally accepted standard technologies and algorithms, business will be forced to employ dual systems in order to ensure secure communications on a global scale. Implementation of these initiatives will represent significant cost to American industry in equipment, software, and other resources.

The U.S. Council's concerns over the Administration's initiatives were expressed in a December 16, 1993 letter to Secretary of Commerce Ronald H. Brown and a March 3, 1994 letter to Vice President Albert Gore. In our letter to Vice President Gore, we said that despite the overwhelming negative public response, the Clipper initiative was still being advanced. Recently, there have been presentations given and press coverage on a new encryption initiative known as Tessera which implements the Capstone chip. Since Tessera has the same fundamental attributes as Clipper, our concerns, as explained below, also apply to Tessera.

As a voice of business, representing large users and vendors of encryption systems, the U.S. Council would like to concentrate its comments on Clipper on three issues of great concern to its members:

(1) competitiveness,
(2) cost to users, and
(3) liability.

1. COMPETITIVENESS

To be competitive in the global marketplace, U.S. companies must be able to sell and integrate into their products, systems that are freely exportable and desirable to users worldwide. Multinationals need secure communications so they can interact not only with their offices but also their suppliers and customers worldwide. For example, in order for financial institutions to be competitive they must use encryption systems, for banking and non-banking applications, that are acceptable worldwide so they can communicate with other financial institutions and their customers around the world. The competitiveness of U.S. companies can be approached from two separate, yet interrelated aspects:

(a) Foreign desirability for chip devices, and
(b) Current export restrictions.

a. Foreign desirability of the key escrow chip

It is unlikely that foreign buyers, especially foreign governments, will want a system developed by the U.S. Government, whereby the U.S. Government holds, or has access to, the keys. Foreign import controls and regulatory requirements for encryption systems present yet another impediment to the foreign sales of Clipper. While there are few obstacles to sales of U.S. encryption products in most foreign countries, some countries require full disclosure of the algorithm or demand that the manufacturers or users deposit the key with the proper authorities. Clipper contains a classified algorithm so it cannot be registered in countries that require disclosure of the algorithm. As the U.S. Government is the holder of, or has access to, the key, a user of Clipper could not deposit the key and it is not known whether the Government will comply with this requirement. Therefore, it seems unlikely that Clipper could be sold in countries that have such requirements.

b. Current export controls

The competitiveness of U.S. companies has suffered long enough under current export control restrictions. DES and RSA use algorithms that are unclassified, widely available around the world, internationally-accepted, implementable in hardware and software, and, most importantly, secure for communications. These encryption systems have been under, and are continually subject to, public scrutiny. As such they have stood the test of time; there have not been any proven successful attempts to break DES or RSA. By protecting economic interests, DES and RSA enhance national security.

Although DES and RSA are widely available and used around the world, they are subject to export control restrictions. Non-U.S. vendors produce and sell these systems in foreign countries where U.S. companies are prohibited from selling because of U.S. export controls. Other encryption systems, based on less powerful algorithms (RC2 and RC4), can be exported on a fast-track export licensing approval process. These weaker systems, however, are less desirable to users of encryption systems. Multinational corporations need to communicate, in a secure manner, with their vendors and customers around the world and should not be prohibited from using the most secure system available. These weaker systems are also less appealing in the international market because foreigners can produce and use the more powerful DES and RSA systems. Moreover, because many foreigners are not subject to the strict export controls that exist in the U.S., non-U.S. manufacturers can sell within their own country and to other countries, where U.S. companies cannot compete. Our competitiveness will only worsen if existing restrictions continue while foreign capability to provide and use powerful encryption systems increases. The logic behind continuing such strict controls on certain U.S. exports, which have wide foreign availability, seems flawed and therefore such controls should be abolished.

2. COSTS TO USERS

There are also substantial operational and administrative costs associated with Clipper. Since Clipper does not interoperate with other encryption systems such as DES, RSA, RC2, and RC4, users will face an additional cost of acquiring the device

that contains the Clipper chip. Although the chip itself is relatively inexpensive (approximately $25 per chip), the cost of implementing it into existing communications systems, or in addition to current systems, will be substantial. The cost to buy the device that contains the Clipper chip will be many times more than the chip itself. Given the substantial investment already made in the installed base of DES and RSA products, the cost to buy additional and different devices is large. Moreover, this is an additional cost that many businesses will essentially be forced to absorb. Corporations that communicate with U.S. Government agencies that use Clipper will also have to use Clipper and thus absorb the costs.

The administrative costs, such as key management, to support differing encryption systems are also substantial. When key management is implemented for only one encryption system, the cost can be held to a minimum. If users need to implement several key management operations, supporting different encryption systems, the costs will be significant.

3. LIABILITY

Lastly, the U.S. Council is very concerned about the issue of liability. Since Clipper is a hardware-based device through which information is encrypted, a compromise of the key will destroy the security of the system and all data contained therein. It is unclear how a company would know if the key has been compromised, who is liable, and who should bear the cost of replacement. Moreover, the consequential damages resulting from a breach in security might be tremendous and possibly unrecoverable. In DES and RSA systems, the user selects his own key; therefore, the keys are not susceptible to being compromised beyond the user's own control. In the case of Clipper, the main keys are assigned during manufacturing, are not changeable by the user and are escrowed with designated agencies. Even though the Government is responsible for developing and holding, or having access to, the keys, it has stated that it would not be liable for any compromise of the keys.

Recommendations

Any encryption policy should be based on an algorithm that is unclassified, implementable in hardware and software, and useable in interconnected networks that are defined by today's global economy. The preferred approach is to use algorithms that are standards (i.e., DES and RSA) and which can be used for digital signature, message authentication, encryption, and key management where the key management system is controlled by its user. Moreover, the encryption system should neither be subject to export control restrictions nor incompatible with existing encryption systems used worldwide. The U.S. Government and the private sector should work together in an open forum to develop an acceptable encryption policy. Our efforts should be coordinated with foreign governments, international institutions, and the international business community to develop a global encryption policy.

Crypto Policy Perspectives

by Susan Landau, Stephen Kent, Clint Brooks, Scott Charney, Dorothy Denning, Whitfield Diffie, Anthony Lauck, Douglas Miller, Peter Neumann, and David Sobel

On April 16, 1993, the White House announced the Escrowed Encryption Initiative, "a voluntary program to improve security and privacy of telephone communications while meeting the legitimate needs of law enforcement." The initiative included a chip for encryption (Clipper), to be incorporated into telecommunications equipment, and a scheme under which secret encryption keys are escrowed with the government; keys will be available to law enforcement officers with legal authorization. The National Security Agency (NSA) designed the system and the underlying cryptographic algorithm SKIPJACK, which is classified. Despite substantial negative comment, ten months later the National Institute of Standards and Technology approved the Escrowed Encryption Standard (EES) as a voluntary Federal standard for encryption of voice, fax, and computer information transmitted over circuit-switched telephone systems.

Underlying the debate on EES are significant issues of conflicting public needs.[1] Every day, millions of people use telephones, fax machines, and computer networks

[1] EES is primarily for use with telephones and fax machines, but this report also addresses the expected extension of escrowed encryption to a broader context than the present Federal standard.

for interactions that used to be the province of written exchanges or face-to-face meetings. Private citizens may want to protect their communications from electronic eavesdroppers. Law enforcement seeks continued access to criminals' communications (under legal authorization). In order to compete in the global marketplace, U.S. manufacturers want to include strong cryptography in their products. Yet national-security interests dictate continued access to foreign intelligence. Both the EES and the controversy surrounding it are but the latest and most visible developments of a conflict inherent in the Information Age. Electronic communication is now an unavoidable component of modern life.

Many times a day people transmit sensitive data over insecure channels: reciting credit card numbers over cellular phones (scanners are ubiquitous), having private exchanges over E-mail (Internet systems are frequently penetrated), charging calls from airports and hotel lobbies (our Personal Identification Numbers (PINs) are easily captured). The problem is magnified at the corporate level. For several years in the nineteen-seventies, IBM executives conducted thousands of phone conversations about business on the company's private microwave network—and those conversations were systematically eavesdropped upon by Soviet Intelligence agents.

IBM's situation is not unique. Weak links exist throughout electronic communications, in networks and in distributed computer systems. Often the vulnerability of communications allows system penetration. Computer systems can be a weak link. Deceptive communications can easily undermine users' confidence in a system. For example, a group of students at the University of Wisconsin forged an E-mail letter of resignation from the Director of Housing to the Chancellor of the University. There can be denials of service because of altered or jammed communications; "video pirates" have disrupted satellite television programs a number of times.

Over the past five years thousands of mainframe computers have been replaced by networked distributed computing systems. This process is accelerating, and that change will only increase the importance of secure electronic communications. The National Information Infrastructure (NII), the "information superhighway", will have an even greater effect. Businesses will teleconnect with customers to sell and bill. Manufacturers will electronically query suppliers to check product availability. Insurance companies, doctors and medical centers will carry on electronic exchanges about patient treatment. The emerging technologies of the Information Age are revolutionizing the ways in which people exchange information and transact business. Much of the information being sent on the NII will be sensitive. Protecting confidentiality, authenticity and integrity in the information infrastructure is extremely important to economic stability and national security.

How can communications security be achieved? A very important part of the solution is cryptography. Cryptography was once the domain of generals and small children, but the advent of the Information Age has sharply increased the public's need for it. Cryptography can help prevent penetration from the outside. It can protect the privacy of users of the system so that only authorized participants can comprehend communications. It can ensure integrity of communications. It can increase assurance that received messages are genuine.

Confidentiality, the benefit most often associated with cryptography, is obtained by transforming (encrypting) data so that it is unintelligible by anyone except the intended recipient. Integrity is a security service that permits a user to detect if data has been tampered with during transmission or while in storage. Closely related to integrity is authenticity, which provides a user with a means of verifying the identity of the sender of a message.

Over the last twenty years several strong cryptographic algorithms[2] have emerged, including the Data Encryption Standard, or DES, and the public key algorithms, Diffie-Hellman and RSA. DES is coming to the end of its useful life with its key size and complexity being overtaken by improvements in speed and cost of computers. Because strong cryptography for confidentiality purposes has the potential to interfere with foreign intelligence gathering, the U.S. government generally does not permit the export of strong cryptography for confidentiality purposes. Strong cryptography can also impede electronic surveillance by law enforcement. Yet the U.S. private sector, from bankers to the future users of the NII, needs strong cryptography.

CRYPTOGRAPHIC ALGORITHMS

The Escrowed Encryption Standard (EES) was proposed as a solution to these conflicting problems, by making available strong cryptography while providing a

[2] Strong cryptographic algorithms are ones which are exceedingly difficult to break by attacks including exhaustive search over the entire key space.

mechanism through which law enforcement could access encrypted communications. But EES raises problems of its own:

(i) Many are uncomfortable with a cryptographic scheme in which the private keys of users are available to the U.S. government,

(ii) Many distrust a scheme where an algorithm for public use is classified,

(iii) Foreign buyers may be unwilling to purchase products that implement the EES, and

(iv) The algorithm is available only in hardware form, increasing costs and decreasing flexibility.

In 1975, the United States proposed DES for the protection of "sensitive but unclassified information" by government agencies. DES, which was designed by IBM, and adopted as a Federal Information Processing Standard (FIPS) in 1977 (in the same series that now includes the EES). It is a private or single-key system and the key used to protect communications between two parties must be known to both parties and kept secret from everyone else.

At the time DES was proposed, it enjoyed a period of controversy in which its keys were characterized as too small and other weaknesses were suspected. Despite this, DES has proven remarkably resistant to public attacks.

At about the same time, academic researchers developed a family of cryptographic techniques that became known as public-key or two-key cryptography. One approach, proposed by Ralph Merkle at Berkeley and refined by Whitfield Diffie and Martin Hellman at Stanford allowed two parties to negotiate a common secret piece of information over an insecure channel. Another, proposed by Diffie and Hellman and realized by Ron Rivest, Adi Shamir, and Leonard Adleman of MIT, made it possible to use a key that was not secret (a public key) to encrypt a message that could only be decrypted by a particular secret key. Conversely, a message transformed by a secret key could be verified as coming from the sender by applying the sender's public key. This second use of public-key technology came to be called a digital signature.

By 1991, the RSA system, which is based on the notion that factoring integers is computationally much more difficult than multiplying them, had become the defacto standard for digital signatures. The list of licensees of RSA digital signature technology[3] read like a computer industry roll-call: Apple, AT&T, DEC, IBM, Lotus, Microsoft, Northern Telecom, Novell, Sun, WordPerfect.

RSA and DES provide the U.S. commercial sector with techniques for achieving confidentiality, integrity and authenticity; for example, Privacy Enhanced Mail (PEM), an Internet standard for secure E-mail, combines them to achieve security. However, with the exception of exporting DES for use by financial institutions or foreign offices of U.S.-controlled companies, the State Department typically refuses export license for confidentiality systems employing the algorithm. Despite this, DES is believed to be the most widely used cryptosystem in the world, except perhaps scramblers used for pay-television. In the United States, the American Banking Association recommends DES whenever cryptography is needed to protect financial data. DES is the cryptographic scheme most often used in commercially available secure telephones.

The export system presents a problem for U.S. industry, all the more so since DES is widely available outside the United States. A March 1994 study by the Software Publishers Association lists thirty-three foreign countries with 152 cryptography-based products using DES.

EMBEDDING CRYPTOGRAPHY

A brief look at communication systems explains the importance of cryptography in achieving security. Telephony is an excellent example. The only way to provide a secure voice path between two telephones at arbitrary locations is to encrypt the words spoken into one and decrypt them as they come out of the other. Public-key cryptography makes it possible for the two phones to agree on a common key known only to them without the mediation of a trusted third party. The users simply establish the call, push a button, and wait a few seconds for the phones to make the arrangements.

In the simplest systems, the users must rely on voice recognition to assure authenticity, just as with unsecured phone calls. If the system must provide authentication to users who do not know one another, some central administration is re-

[3] RSA is patented in the U.S.

quired to issue cryptographic credentials by which each phone can recognize the other.

Currently, secure telephones are expensive. In addition to the cryptographic devices, a secure phone must include a voice digitizer to convert speech to a form in which it can be encrypted and a modem to encode the digitized signal for transmission over the phone line. As a result, the least expensive secure phones cost over a thousand dollars apiece.

Securing communications for computers in a distributed system presents different problems. There is no analogue of voice recognition. If authentication is to be available, it must be done by formal cryptographic procedures. This requires the computers to identify people or machines through long-term keys. The relationship between telephones, even secure telephones, is conceptually simple: they set up calls and transmit sound. The relationship between computers in a distributed system is considerably more complex: machines routinely share files and execute programs for each other. These wedded interactions complicate the process of protection and make computer break-ins difficult to prevent.

Systems owners are typically unwilling to make substantial investments in hardware or software for security purposes, although they may be willing to pay some premium for products that contain integrated security features. Many vendors see software as the least expensive means of adding cryptographic security features to their products.

A secure mail system like PEM is the workstation analogue of a secure telephone; it encrypts and decrypts mail so the user can correspond privately. Unfortunately, a software implementation of PEM is vulnerable to penetration of the program including the compromise of its long term keys. One of the ways in which such penetrations occur is through the implanting of modified programs or other data into the user's working environment. Without trustworthiness, cryptography embedded in an application or in the operating system is no panacea.

LAW ENFORCEMENT

Technology causes a constant rearrangement in the relationship between the criminal and the law. The advent of telecommunications enabled criminals to execute their plans more covertly. Once law enforcement learned how to listen in, officials could do so without placing themselves in danger. Wiretapping is a tool that diminishes the value of communications to criminals cryptography potentially counters this.

Current wiretap law dates from the 1968 Omnibus Crime Control and Safe Streets Act; Title III of the Act established the basic law governing interceptions in criminal investigations. In 1978 the Foreign Intelligence Surveillance Act established the national-security counterpart to Title III, authorizing electronic surveillance for foreign intelligence.

Title III requires a court order for the installation of a wiretap (as do most FISA intercepts). For Title III orders there must be probable cause to believe that the targeted communications device—whether phone, fax, or computer—is being used to facilitate a crime, which must be one of those enumerated by the law. Thirty-seven states also have statutes authorizing wiretaps; by law, the state requirements must be at least as restrictive as the Federal statute.

Since 1968, when Title III was passed, there have been approximately nine hundred Federal and state wiretaps annually. In data released by the Administrative Office of the U.S. Courts, between 1968 and 1992, the average annual number of incriminating conversations intercepted has remained between two and four hundred thousand. In 1992, the average cost of installing a wiretap and subsequently monitoring it was $46,492.

The law enforcement community views wiretaps as essential. Such surveillance not only provides information not obtainable by other means, it also yields evidence that is considered extremely reliable and probative. According to the FBI, organized crime has had severe setbacks due to the use of wiretap surveillance. The FBI believes the tool is critical for drug cases. Wiretapping is an important investigative technique in cases of governmental corruption and acts of terrorism.

The importance of wiretap surveillance was the reason for the Digital Telephony Proposal, which was developed by the FBI and submitted to Congress in 1992. To ensure that the government's ability to intercept communications is not curtailed by the introduction of advanced digital switching technology, this proposal requires providers of electronic communication services to design their switches accordingly. Major members of the computer and communications industries, including AT&T, Digital, Lotus, Microsoft and Sun, strongly opposed the proposal, and there were no

Congressional sponsors. A revised proposal was recently submitted for consideration.

The Digital Telephony Proposal concerns access to communications, but law enforcement is also concerned about its ability to understand those communications after interception. Off-the-shelf encryption technology may be an easy way for lawbreakers to foil criminal investigative work. Members of the law-enforcement community view EES as a solution that provides the public with strong cryptography while not compromising investigators' ability to comprehend legally intercepted communications.

NATIONAL SECURITY

Foreign access to cryptography of even moderate strength poses a problem for U.S. intelligence. Those who think about vulnerabilities from the viewpoint of security typically regard strong encryption of each message as the only barrier to communications intelligence. However, a message cannot be analyzed until it has been located. Locating the traffic of interest is as important a problem as any. Even encryption that is too weak to resist concerted attack can multiply the cost of targeting traffic several-fold.

The growth of communications intelligence in this century has been accompanied by a similar growth in techniques for protecting communications, particularly cryptography. Nonetheless the communications intelligence product is now better than ever. In the recent past, there has been migration of communications from more secure media such as wirelines or physical shipment to microwave and satellite channels; this migration has far outstripped the application of any protective measures.

But while the United States may be the greatest beneficiary of communications intelligence in the world today, it is also its greatest potential prey. The protection of American communications against both interception and disruption is vital to the security of the country.

When DES was adopted as a government standard in 1977, cryptographic protection of substantial quality became available in both hardware and soft-ware packages. With hindsight, some in the intelligence community might consider the public disclosure of the DES algorithm to have been a serious error. DES-based equipment became available throughout the world; cryptographic principles revealed by studying the algorithm inspired new cryptographic designs; and DES provided a training ground for a generation of public cryptanalysts.

EXPORT CONTROL

National-security experts argue that export control is essential if the U.S. is to protect its communications without affording protection to the rest of the world. Export-control policy seeks to limit foreign accessibility to strong cryptography. Internet availability of strong cryptography notwithstanding, many security experts believe that the export control policy is working. They argue that foreign organizations that are concerned about protecting their information from sophisticated intercept are not likely to download an encryption program from the Internet. Others disagree, and believe that the only real effect of present export-control policy is to ship U.S. jobs overseas. Many complain that export control has had a chilling effect on American business by making U.S. products less competitive.

Export-control policy on cryptography has complicated development of secure systems. An example is provided by the Digital Equipment's Distributed System Security Architecture (DSSA), which DEC spent many years and many millions of dollars developing. In planning the system, Digital sought to make a product which would pass government export controls for cryptography. In particular, in designing DSSA Digital engineers carefully separated authentication from confidentiality. They began building two distinct versions of the product, a domestic one with authentication and confidentiality, and one for export, with authentication only. This additional complexity slowed the work. A Digital senior manager familiar with the program asserted that the delays associated with attempts to meet export restrictions were a significant factor in Digital's decision to abandon DSSA.

Cryptography is not the only American product subject to export control. Striking a balance between economic strength (by opening markets for U.S. companies), and protecting national security (by restricting the sale of military technology) requires making complex choices. What differentiates this conflict from, say, the exportability of supercomputers, is that equivalent cryptographic products are available for sale internationally. Opponents of cryptographic export controls argue that U.S. vendors are penalized while cryptographic products proliferate. Proponents of these controls argue that the most serious threat to foreign intelligence gathering comes not from stand-alone products that constitute most of the market, but from well-integrated,

user-friendly systems in which cryptography is but one of many features. From this perspective, it is essential to control export of the commodity, desktop hardware and software with integrated cryptography. The U.S. is the pre-emininent supplier of such products.

National-security experts have argued that removal of U.S. export controls on cryptography would result in the imposition of foreign import controls; they point to France, which does not permit the use of encryption without governmental registration of the algorithm. In recent years, the policy of the U.S. government is to oppose trade restraints, so this contention; something of an about-face. It is speculative. At present, no Western European governments other than France restrain the import of cryptographic products, and only a few Asian governments do so.

The EES may have an indirect impact on the export of computer equipment. Export of key-escrow equipment will be permitted, but both the secrecy of the algorithm and the U.S. government's possession of keys may dampen the enthusiasm of prospective foreign buyers. In order to build products for both the domestic and export markets, computer vendors might need to support two sets of cryptographic algorithms.

THE RIGHT TO PRIVACY

If law enforcement and national-security interests argue against the availability of strong cryptography without key escrow, other traditions of the U.S. argue strongly in its favor. The right to privacy, the "right to be left alone" is fundamental to American life. Civil libertarians view the availability of strong cryptography as necessary to the ability to communicate in privacy.

Protecting American's privacy rights is a constant struggle. Private industry, including credit bureaus, insurance companies, and direct marketers, collects a vast amount of information about individuals. The proliferation of electronic databases has only exacerbated the problems Congress attempted to ameliorate twenty-four years ago, when it passed the Fair Credit Reporting Act. Despite abuses by the private sector, civil-liberties groups view government abuse of privacy with much greater concern. In its attempt to ensure the safety of its citizens, the government can overstep boundaries of the rights of the individual. One does not have to look far back in the nation's history to find egregious examples of such abuse.

Based on information illegally supplied by the Census Bureau, one hundred and twelve thousand Americans of Japanese ancestry were put in internment camps during World War II. During the nineteen-sixties, the FBI regularly taped conversations of many civil rights leaders, including Martin Luther King. The 1974 Senate Select Committee to Study Governmental Operations found numerous examples of the NSA abuse of privacy rights of private individuals. As a direct result of these activities, legislative, executive order and regulatory provisions were instituted with the intent of eliminating future such occurrences.

Privacy rights are one of the individual's most potent defenses against the state. Privacy rights of the individual are embedded in the Fourth and Fifth Amendments. Supreme Court Justice Louis Brandeis said it eloquently in his dissent on the Olmstead wiretapping case,

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and his intellect * * * They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized man * * *[4]

Privacy, however, is not always deemed absolute. Sometimes privacy is traded for convenience. Americans are captured on video recordings as we shop; we leave behind electronic chronicles as we charge phone calls. We pay for milk and bread via an ATM withdrawal at the supermarket, and we leave a record of our actions where five years ago we would have left a five-dollar bill. Sometimes it is traded for safety. Each day hundreds of thousands of Americans pass through metal detectors to get on airplanes. Most people consider those intrusions of privacy well worth the assurance of greater public safety.

---

[4] *Olmstead* v. *United States,* 277 U.S. 438, 1928, pg. 752.

CRYPTOGRAPHY POLICY

Civil-liberties groups argue that constitutional protections need to keep pace with new technology. Their concern is that governmental attempts to limit the use of cryptography, whether through force of law, or through more subtle efforts such as market domination, can result in the foreclosing of privacy protection choices.

Concern over control of cryptography first arose when cryptography became an active area of research for academia and business. There were conflicts over which Federal agencies would fund non-governmental cryptography research, and whether such work might be subject to some form of prior restraint on publication.

In response to these difficulties, the American Council on Education convened a study group, which presented a set of voluntary guidelines for prepublication review of research papers in cryptography. The National Security Agency and the National Science Foundation worked out an agreement by which both agencies would fund cryptographic research. Research now flourishes in both domains.

Several years later, President Reagan issued National Security Decision Directive 145 (NSDD–145), establishing as Federal policy the safeguarding of sensitive but unclassified information in communications and computer systems. NSDD–145 stipulated a Defense Department management structure to implement the policy: the NSA, the National Security Council and the Department of Defense. There were many objections to this plan, from a variety of constituencies. Congress protested the expansion of Presidential authority to policy-making without legislative participation. From the ACLU to Mead Data Central, a broad array of industrial and civil-liberties organizations objected to Department of Defense control of unclassified information in the civilian sector.

In 1987 Congress sought to clarify the issue with the Computer Security Act, which assigned to the National Bureau of Standards (now the National Institute of Standards and Technology, or NIST) "responsibility for developing standards and guidelines to assure cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate."

Civilian computer security standards were to be set by a civilian agency. But seven years later both civil-liberties and industrial groups feel NSA is more involved in civilian standards than the Computer Security Act mandated. They point to the NSA-designed digital signature standard (DSS) and the cryptographic algorithm SKIPJACK that underlies EES. Concerns over national-security involvement in civilian matters, as well as concerns over the government plan to escrow keys of private users have led such civil-liberties groups as the ACLU and Computer professionals for Social Responsibility to oppose EES.

EES AND PRIVACY

Advocates of EES claim the availability of strong cryptography will provide Americans with better and more readily available privacy protection than they currently enjoy. They observe that no one will be forced to use it, and that other forms of encryption will be allowed. Opponents believe the potential for abuse by the government makes EES a danger not to be risked, and counter that if a large Federal agency like the IRS adopts EES, then electronic filers who choose to secure their transmissions may have to use EES. This would have the impact of making the voluntary standard the de facto national one.

There is no question that the market impact of the Federal government can be huge, although recent experience illustrates that the government's ability to influence the computer communication market is not always successful.[5] Adoption of EES, as a standard, voluntary or otherwise, decreases the chance there will be competing systems available. Indeed the true success of EES, as measured by law enforcement's continued ability to decrypt intercepted conversations, can only come at the expense of (widespread use of) competing systems for secure telecommunications.

Proponents respond that privacy protection will be better than ever. Should the government illegally tap a communication, the escrowed system will leave an electronic audit trail, and make the illegal interception easier to uncover than it is at present. Reminding us of the abuses of Watergate and the revelations of the Church Committee, civil-liberties groups contend that the NSA should not be building government trap-doors into the civilian communications infrastructure.

---

[5] The failure of the GOSIP initiative, an attempt to mandate procurement of computer communication protocols that conform to the 150 OSI standards, is one such example.

EES AND THE COMPUTER INDUSTRY

Meanwhile EES presents other problems for the computer industry. The government's attempt to create strong cryptography that would not hinder law enforcement's abilities to comprehend legally intercepted conversations led to a hardware solution. Industry prefers software implementations for a number of reasons. They are cheaper, and they offer a flexibility that hardware does not.

The industry has already made substantial investments in DES and RSA solutions for secure systems. In lots of ten thousand, Clipper chips will cost approximately $15; industry experts contend that this translates to a finished product with escrowed encryption capabilities costing about sixty dollars more than one without. From a vendor viewpoint, hardware encryption provides greater security but does so at much greater expense than software. It is not clear that prospective purchasers are willing to pay for this increased security.

THE BROADER POLICY ISSUES

In the full report, we discuss in detail the various policy and technical concerns surrounding cryptography. The problems of communications security and its cryptographic solution are technical ones, but the issues are much broader. They deserve careful and thoughtful public debate. We raise questions here and in the full report. Answers will take longer.

It took the Supreme Court nearly forty years to expound on the privacy of telephone communications. In the *Olmstead* case in 1928, the Supreme Court held that wiretapping evidence did not need court authorization. Over the next four decades, the Court slowly created a penumbra of privacy for telecommunications. Finally, in 1967, in Katz versus the United States, the Court held that a phone call in even so public a place as a phone booth was deserving of privacy—it could not be tapped without prior court authorization. Computer communications differ from the telephone, but it is likely that the public's embrace of this medium will be considerably more rapid than the acceptance of the earlier technology. How will law and policy for the protection of electronic communications evolve? Is there an absolute right to communications privacy?

Members of the law enforcement community believe that the widespread use of encrypted telecommunications (especially phone calls) will interfere with their ability to carry out authorized wiretaps. Is this a problem that needs a solution? Should cryptographic solutions for communications security include authorized government access for law enforcement and national security purposes?

What will happen if criminals use cryptography other than EES? The Digital Telephony proposal involves investment in the telephone infrastructure in order to ensure that court-authorized wiretaps can be carried out. These wiretap capabilities will be less useful if communications are encrypted. What is the relationship between Digital Telephony and EES? Will there be any future attempt to outlaw alternative forms of cryptography?

What would the success of escrowed encryption mean? Would it simply mean government use of EES-type products? Or would it mean a much more widespread use of EES products? Would it mean the availability of EES-type products to the exclusion of all else?

We are experiencing fundamental transformations in the way that people and organizations communicate. The very infrastructure of the nation is changing. The question we need to address is: How should we interpret the Fourth Amendment,

> The right of the people to be secure in their persons, house, papers and effects against unreasonable searches and seizures shall not be violated; and no warrants shall issue but upon probable cause * * *

for the Information Age?

DESCRIPTION OF AUTHORS

Susan Landau is Research Associate Professor at the University of Massachusetts. She works in algebraic algorithms, which has applications to cryptography.

Stephen Kent is Chief Scientist-Security Technology for Bolt Beranek and Newamn Inc. For over 18 years, he has been an architect of computer network security protocols and technology for use in the government and commercial sectors.

Clinton C. Brooks is an Assistant to the Director of the National Security Agency. He is responsible for orchestrating the Agency's technical support for the government's key escrow initiative.

Scott Charney is Chief of the Computer Crime Unit in the Criminal Division in the Department of Justice. He supervises five federal prosecutors who are responsible for implementing the Justice Department's Computer Crime Initiative.

Dorothy E. Denning is Professor and Chair of Computer Science at Georgetown University. She is author of "Cryptography and Data Security" and one of the outside reviewers of the Clipper system.

Whitfield Diffie is Distinguished Engineer at Sun Microsystems. He is the co-inventor of public-key cryptography, and has worked extensively in cryptography and secure systems.

Anthony Lauck is a Corporate Consulting Engineer at Digital Equipment and its lead network architect since 1978. His contributions span a wide range of networking and distributed processing technologies.

Douglas Miller is Government Affairs Manager for the Software Publishers Association.

Peter G. Neumann has been a computer professional since 1953, and involved in computer-communication security since 1965. He chairs the ACM Committee on Computers and Public Policy and moderates the Risks Forum.

David L. Sobel is Legal Counsel to the Electronic Privacy Information Center (EPIC). He specializes in civil liberties, information and privacy law and frequently writes about these issues.

Yankelovich Partners

3822 Campus Drive, Newport Beach, CA 92660

Memorandum

To: Data users
From: Hal Quinley
Date: March 7
Subject: Time/CNN poll

Here are the results of the latest Time/CNN poll conducted on March 2-3, 1994. The survey was conducted by telephone among 600 adult Americans. The sampling error is plus or minus 4%.

The De-encryption Chip Issues
(March 2-3, 1994)

	Total %
19. Which of the following do you think is more important?	
Protecting the ability of police and other government officials to catch criminals by listening to phone calls	29
(Or,) Protecting the ability of private citizens to prevent anyone, including the police, from listening to their phone calls	66
Not sure	5
20. It has been proposed that a computer chip be installed in every telephone, computer modem and fax machine. The government would be able to tap into these devices and listen to messages if a judge permits it. Do you favor or oppose giving the federal government this authority?	
Favor	18
Oppose	80
Not sure	2

TABLE 45

Q13. WHICH IS MORE IMPORTANT IN REGARDS TO LISTENING IN ON PHONE CALLS:

	TOTAL	PARTY ID: REPUBLICAN	PARTY ID: INDEPENDENT	PARTY ID: DEMOCRAT	SEX: MEN	SEX: WOMEN	REGION: NRTH EAST	REGION: MID-WEST	REGION: SOUTH	REGION: WEST	AGE: 18 - 34	AGE: 35 - 49	AGE: 50 - 64	AGE: OVER 64	INCOME: UNDR $20K	INCOME: $20K TO $35K	INCOME: $35K TO $50K	INCOME: OVER $50K	RACE: WHITE	RACE: BLACK	RACE: OTHR
UNWEIGHTED TOTAL	600	162	215	191	300	300	126	150	204	120	204	191	97	100	121	163	143	120	505	47	41
TOTAL RESPONDENTS	600	183	214	203	286	314	126	146	206	122	229	155	114	93	142	178	132	108	494	86	34
	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
PROTECTING THE ABILITY OF POLICE AND OTHER GOVERNMENT OFFICIALS TO CATCH CRIMINALS BY LISTENING TO PHONE CALLS	171	55	57	50	71	101	38	49	58	30	63	40	38	30	42	47	29	42	147	14	10
	29%	30%	27%	25%	25%	32%	27%	34%	28%	25%	28%	26%	33%	31%	30%	27%	22%	40%	30%	21%	30%
PROTECTING THE ABILITY OF PRIVATE CITIZENS TO PREVENT ANYONE, INCLUDING THE POLICE, FROM LISTENING TO THEIR PHONE CALLS	399	94	130	138	203	193	83	91	136	86	162	110	73	50	87	125	101	56	322	51	21
	68%	51%	70%	68%	72%	62%	66%	62%	67%	70%	71%	71%	64%	54%	61%	71%	77%	53%	65%	77%	64%
NOT SURE	29	5	7	15	5	20	8	5	10	6	4	5	3	13	12	2	2	5	25	1	1
	5%	3%	3%	7%	3%	6%	6%	4%	5%	5%	2%	3%	3%	14%	9%	2%	1%	5%	5%	2%	4%
SIGMA	599	183	212	202	285	313	126	145	205	122	229	155	113	93	141	175	131	104	494	66	31
	100%	100%	100%	100%	100%	100%	99%	100%	100%	100%	101%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

TABLE 44

Q20. FAVOR OR OPPOSE GIVING THE FEDERAL GOVERNMENT THE AUTHORITY TO TAP INTO PHONES, MODEMS, AND FAX MACHINES THROUGH A COMPUTER CHIP IF PERMITTED BY A JUDGE

		PARTY ID			SEX		REGION				AGE				INCOME				RACE		
	TOTAL	REPU-BLI-CAN	INDE-PEN-DENT	DE-MO-CRAT	MEN	WO-MEN	NRTH EAST	MID-WEST	SOU-TH	WEST	18 - 34	35 - 49	50 - 64	OVER 64	UNDR $20K	$20K TO $35K	$35K TO $50K	OVER $50K	WH-ITE	BL-ACK	OTHER
UNWEIGHTED TOTAL	600	163	215	191	300	300	126	150	204	120	204	191	97	100	121	169	145	120	505	47	41
TOTAL RESPONDENTS	600 100%	153 100%	214 100%	202 100%	286 100%	314 100%	126 100%	146 100%	206 100%	122 100%	229 100%	155 100%	114 100%	95 100%	142 100%	175 100%	122 100%	108 100%	494 100%	66 100%	34 100%
FAVOR	108 18%	27 18%	45 21%	32 16%	46 16%	63 20%	25 20%	29 20%	33 16%	21 17%	51 22%	27 17%	16 14%	14 15%	26 18%	33 19%	19 14%	28 25%	97 20%	6 9%	6 17%
OPPOSE	481 80%	126 82%	169 79%	163 80%	236 83%	245 78%	95 76%	115 79%	171 83%	100 82%	176 77%	127 82%	95 83%	80 84%	111 78%	141 81%	112 92%	78 75%	390 79%	59 89%	27 82%
NOT SURE	10 2%	-	-	7 4%	4 1%	7 2%	6 5%	2 1%	2 1%	1 1%	3 1%	2 1%	3 2%	1 1%	4 2%	1 1%	1 0%	1 1%	8 2%	1 2%	1 2%
SIGMA	599 100%	153 100%	213 100%	202 100%	285 100%	313 100%	125 101%	145 100%	205 100%	122 100%	229 100%	155 100%	114 99%	95 100%	141 100%	175 101%	131 99%	106 101%	494 101%	66 100%	33 101%

Questions and Answers

Answers to Questions From Senator Leahy to Assistant Attorney General Jo Ann Harris

Question 1. What is the number of people who will have access to the key escrow facilities within the Commerce and Treasury Departments? What is the number of people with access to those keys that have been released pursuant to court order?

Answer 1. To begin with, it must be understood that the key-escrow databases will be held in encrypted form and that the escrow agents will be incapable of decrypting those databases. Nevertheless, both NIST and Treasury will strictly limit the number of individuals that have access to the key-escrow databases, with the objective of keeping that number to the minimum necessary to meet the requirements of the system, including the need for a 24-hour response capability. In each agency, the number of individuals with such access is expected to be no more than about a dozen, and, in each case, fewer than that number are expected to be involved in the chip programming process. Moreover, all such individuals will hold national security clearances at least to the Secret level.

We understand the second question as asking the number of persons who will have access to the key components at the agency to which the components have been released for use in conjunction with lawfully authorized electronic surveillance. We cannot, of course, provide a precise number of the persons at, for example, a field office of the Drug Enforcement Administration, who might be present when a key component is received from an escrow agent. In this regard, however, it should be remembered that the key components are stored and transmitted in encrypted form and that the encrypted components can only be decrypted, combined, and used by the decrypt processor. Therefore, the receiving law enforcement agency has no access to the unencrypted key. Consequently, we believe that what is important is not the number of persons at the receiving law enforcement agency who may lay eyes on an encrypted string of 80 bits, but, rather, the rigid controls over the conduct of electronic surveillance that may require decryption of key escrow-encrypted communications.

Question 2. Can an escrow agent exercise discretion in the release of key information? Can they refuse an inappropriate request?

Answer 2. The escrow agents are not in a position to exercise discretion regarding the propriety of releasing key components in response to properly submitted requests, because they should not substitute their judgment regarding the propriety of decrypting communications for the judgment of the court that has authorized the interception of such communications. The procedures for key component release to government agencies are intended to permit escrow agents to respond promptly to requests submitted in proper form and to maintain clear, auditable records of the transaction.

A properly submitted request will include, among other things, identification of the agency and individuals making the request, identification of the source of the authorization to conduct electronic surveillance, and specification of the termination date of the authorized surveillance period. Federal agency requests for releases under Title III or FISA will be followed by an attorney's confirmation of authority to conduct electronic surveillance; State or local requests are to be submitted by the principal prosecuting attorney of the State or political subdivision involved. A key escrow agent may not, of course, release a key component in response to a request not meeting the requirements for submission, including, for example, one that does not specify the source of the authorization.

Question 3. What is the process for auditing the activities of the escrow agents and use of the keys?

Answer 3. Auditing will be possible at various stages of the process, as well as in retrospect. Thus, for example, after being advised of a key component release request, the Department of Justice will make necessary inquiry to be assured that the relevant Federal, State or local authorities have been authorized to conduct electronic surveillance for criminal investigative purposes, or that relevant Federal authorities have been authorized to conduct electronic surveillance under FISA. (At least at the outset, such inquiry will be made in all cases.) Key component releases will require confirmation of receipt of the key components by the intended recipient agency.

The fully developed key escrow database system will provide permanent electronic records of transactions, particularly the details of releases of key components, with secure audit capabilities built in. The compliance of the key escrow agents will be

subject to inspection, both by representatives of the Department of Justice and by inspection personnel within their own organizations, to verify the relationship between each key escrow component release and a properly submitted release request and receipt of a certification of termination of decryption capability in conjunction with the end of the authorized period of electronic surveillance.

Later versions of the decrypt processor will automatically terminate decryption capability no later than the end of the period of authorized electronic surveillance. In the prototype version, decryption capability is terminated manually. That termination can easily be confirmed by physical inspection, particularly since, in the early stages of the program, the decrypt processors are expected to be centrally held.

These methods of confirming the integrity of the system are over and above those procedures normally associated with electronic surveillance. For example, electronic surveillance logs can be reviewed to confirm that a request for key component release truly was associated with the particular wiretap on which the requester relied.

Question 4. Situations have arisen where the government has created systems that were only supposed to be used for one purpose but have been permitted to be used for others. What protections are in place to make sure that the key escrow databases held by the escrow agents are never used for any purpose other than to decrypt messages pursuant to a lawful court order?

Answer 4. Each of the key escrow agents administers a database that comprises, essentially, two groups of data: a series of chip unique ID numbers and, for each chip unique ID number, a string of 80 bits that is stored only in encrypted form. Those databases contain no personal information associated with individuals who may own or use devices equipped with the particular chips; hence, the key escrow databases are not susceptible to the kinds of misuse to which databases of personal information might be subject.

Nonetheless, the Administration recognizes that it is crucial to ensure that key components contained in those databases are only made available to government agencies for use in conjunction with lawfully authorized electronic surveillance. For that reason, rigorous procedures for release of key components have been approved (copies of which are attached), and extremely strict database handling and processing technology and procedures have been implemented and are being further refined.

It should also be noted that key components will be provided requesting government agencies upon their certification of authority to conduct electronic surveillance; their actual submission of a court order will not be necessary.

Question 5. How will the released escrow keys be transported to the law enforcement agency requesting them? What safeguards will be used when transporting the escrow keys?

Answer 5. Key components are stored and transmitted to law enforcement agencies in encrypted form; they can be decrypted and combined only within the decrypt processor. Thus, neither the escrow agents, nor personnel at the law enforcement agency, will see the actual key components. Normally, the key components will be transmitted electronically. Initially, for use in the prototype version of the decrypt processor, they will be hand-carried by representatives of the respective escrow agents, to be manually entered (in encrypted form) into the processor. More advanced versions of the decrypt processor will be able to receive input of the key components electronically transmitted directly from the escrow facility.

Question 6. If an escrow location is compromised, all chip data contained there is compromised with what could be devastating consequences for U.S. Government and private sector entities using security devices with Clipper Chip. Do you anticipate that these locations will become targets of opportunity for any criminal or terrorist organization? What back-up or physical security measures are envisioned? If multiple copies of the keys are kept, does this increase the threat of compromise?

Answer 6. The key escrow system has been designed so that knowledge of one key component provides no information regarding the other key component, nor regarding the entire unique key. Moreover, the key components are themselves maintained in encrypted form, so that a person with access to a key component database does not even know the actual key components. Notwithstanding these safeguards built into the system, physical security of the key-escrow databases is a matter of fundamental concern, and security procedures for handling and storing the databases take full account of that concern. The key-escrow databases are to be held under the kinds of protections accorded the most sensitive kinds of national security information. Back-up database capabilities will be maintained, so that escrow agents will be able to respond in a timely fashion even if the primary site is, for example, incapacitated by a fire or power outage. The back-up capabilities are subject to the same levels of protection as the primary systems.

Question 7. A decrypt device will receive an electronic transmittal of the two key halves from the escrow agents. The decrypt device will then be able to decrypt the intercepted message, until the wiretap authorization ends, when it will automatically turn itself off. According to Department of Justice testimony at the May 3, 1994 hearing, one of these decrypt devices has been built. How many more of these devices do you expect to be built? Will the decrypt devices be maintained in the central secure facility? If so, who will maintain custody of the devices and how will they be distributed to the law enforcement agencies that need them?

Answer 7. Termination of a decrypt processor's ability to decrypt communications using a particular key-escrow chip is a fundamental protection built into the system, and law enforcement agencies that have received key components will be required to certify such termination. In the prototype model of the decrypt processor, that termination is effected manually; automatic termination will be available in later versions.

The number of decrypt processors that will ultimately be produced will probably be in large measure a function of the number of key-escrow equipped devices in use throughout the country and the number of times key-escrow encryption is encountered in the course of wiretaps. For the foreseeable future, it is likely that decrypt processors would be centrally held by the FBI, to be made available for use in the field on an as-needed basis.

Question 8. The objective of the key escrow encryption system is to provide "real-time" electronic surveillance rather than recording and post-processing of targeted encrypted communications. How will this be accomplished with only one decrypt device in the event that encrypted communications are intercepted over more than one wiretap?

Answer 8. As noted in the previous question, the key escrow system is still in its beginning phases and, therefore, the number of decrypt processors is, at the moment, necessarily limited. This condition will change over time. However, the fact that there is only one decrypt processor currently available does not mean that it can only be used in support of one wiretap at a time. The decrypt processor is capable of holding within its memory up to one hundred keys. Therefore, while it can only decrypt one communication at a time, it can readily be shifted from one wiretap to another as needed. Even wiretaps conducted at different locations can be accommodated by retransmitting an encrypted intercepted communication from the primary monitoring location to the location of the decrypt processor.

Question 9. The Attorney General has selected NIST and the Automated Systems Division of the Treasury Department as the government agencies entrusted with safeguarding the keys because they could handle sensitive material in computer form and could respond quickly to requests for the keys.

- Is it correct that other government agencies could also satisfy this criteria?
- Could one or both of the escrow agents be non- government, private sector entities?

Answer 9. Of course, other government agencies could meet the requirements for satisfactory service as key component escrow agents. Some of those agencies, however, might not be perceived as sufficiently independent of law enforcement or national security entities, or may otherwise not be considered as capable as the two selected agencies.

With respect to the second question, it may not be necessary that both escrow agents be government entities. However, should a private entity serve as an escrow agent, there may be additional complexities regarding, among other things, the terms of any contract under which the entity serves; provisions to ensure the continued corporate existence of such an entity; the entity's ability to accord the database the necessary physical security; the entity's ability to staff the system with sufficient numbers of appropriately cleared personnel; and its ability and willingness to respond to key component requests from all authorized law enforcement agencies, State and local as well as Federal.

Question 10. Can the Attorney General change the escrow agents after the initial selection? How can the government be prevented from moving the escrow responsibilities to a more pliable escrow agent, if one of the agents refuses to turn over the keys?

Answer 10. The Attorney General can designate an alternative escrow agent, and, as part of its continuing review of ways to make the system even better, the Administration is considering whether there should be at least one escrow agent not within the Cabinet Departments. Designation of an alternative escrow agent would entail substantial complexities, not to mention considerable costs associated with establishing the necessary capabilities in the new agency. It will not be done lightly, nor could it be done without a good deal of publicity. Replacement of one escrow

agent with another would involve even greater complexities, since it would require the first to convey to the second its entire database to permit continuity in the handling and auditing of the database.

The second question seems to hypothesize an escrow agent's refusal to release a requested key component, followed by a retaliatory transfer of escrow agent responsibilities to a agency deemed less likely to be recalcitrant. The short answer is that such a replacement, while theoretically possible, could abrogate the integrity of the system and would very likely undermine public confidence in it. Moreover, the Clinton Administration would not accept as an escrow agent an entity that would not fully comply with the protections built into the system. Indeed, regardless of the administration in power, the fact that such a change would be logistically very difficult and could only be done in a very public fashion makes it an extremely unlikely scenario.

Question 11. In explaining the procedures the escrow agents must follow to safeguard the keys, the Attorney General stated "the procedures do not create, and are not intended to create any substantive rights for individuals intercepted through electronic surveillance." Does this, in effect, give the escrow agents immunity from liability for mishandling the keys? Does this give the right incentives to the escrow agents about safeguarding the keys? What are the current available remedies for mishandling the keys?

Answer 11. The language to which you refer is part of the final paragraph in each of the three published sets of procedures for release of key components under, respectively, Title III, the Foreign Intelligence Surveillance Act (FISA), and State criminal wiretap statutes.

The language is intended to make clear that the procedures themselves do not create any rights for individuals whose communications have been intercepted and for whose devices key components have been made available to government agencies. On the other hand, neither does the language abolish any rights that may otherwise exist by statute or at common law. It is not intended to be, nor could it serve to immunize the Government or its agents from liability for inappropriate release of escrowed key components if there is some basis in law for imposing liability on such persons.

In this regard, it is important to bear in mind the fundamental interest at issue; namely, the protection of the privacy of communications. Release of key escrow components to permit decryption is an adjunct to the interception of communications and the acquisition of the contents thereof—much like arranging for translation of communications occurring in a foreign language. The privacy interest in the communication continues to be protected by the Fourth Amendment and by the relevant statutes—Title III, FISA, or the individual State statutes. Unauthorized electronic surveillance is a Federal felony offense, regardless of whether the intercepted communications are encrypted.

While key components must only be released to proper recipients and under appropriate conditions, there should be no confusion about the fact that an individual's privacy interest inheres in his or her communications. If key components are released to a government agency entitled to intercept communications encrypted with a chip for which those components form the chip unique key, a departure from some technical aspect of the key release procedures will not—and should not—render either the intercept or the decryption unlawful. If key components are for some reason released to an entity not entitled to receive them, but are not used in conjunction with a communications intercept, the individual will not have suffered an invasion of his or her communications privacy. It is not clear under what, if any, circumstances mere release of one or even both keys might create civil liability, if that release does not facilitate an unlawful electronic surveillance.

Question 12. Should the U.S. government be prepared to make a strong warranty to the American public about the security of the key escrow system? Could this warranty be in the form of stiff penalties for breaches of the escrow procedures and indemnification for those whose chips are compromised due to failures in the security of the escrow system?

Answer 12. The Clinton Administration has already given strong assurances to the American public about the security of the key escrow system and will continue to do so. It is not clear whether public perceptions about key-escrow encryption would be materially affected by either imposition of penalties for breach of escrow procedures or indemnification of persons whose chips have been compromised through escrow system security failures.

It may, however, be useful to make a few points regarding those possible approaches. First, as noted in the answer to the preceding question, the privacy protection attaches to the communication, not merely to the keys needed to decrypt that communication. Federal law already imposes severe penalties (both civil and

criminal) for unlawful interception of communications, and, therefore, no additional penalties are needed in that regard.

Second, some persons speak of a variety of circumstances as constituting a "compromise" of a key escrow encryption chip. It is not clear that mere release of key components for a particular chip to persons not authorized to intercept communications encrypted with that chip necessarily means that the chip has been compromised. The key components alone do not permit decryption of communications encrypted with the particular chip; that process requires, as well, access to a decryption capability. Moreover, decryption of communications requires access to the communications themselves, the privacy of which is subject to the protections of the Fourth Amendment and relevant statutes.

Question 13. Should there be civil or even criminal liability for wrongfully disclosing any of the component keys to the key escrow chips? If not, why not?

Answer 13. As noted in the answers to the two preceding questions, the rigorous statutory protections against unauthorized electronic surveillance and against unauthorized disclosure of electronic surveillance already provide both civil and criminal penalties for the unlawful interception of communications and the unauthorized disclosure of the contents of lawfully intercepted communications. (See 18 U.S.C. §§2511, 2517, and 2520.) Release of escrowed key components would, at most, facilitate understanding of the contents of intercepted communications. An individual's willful or reckless release of key components in a manner not consistent with the operative procedures would likely be subject to administrative action. Separate criminal or civil penalties do not appear to be needed.

Question 14. The Department of Justice testified at the May 3, 1994 hearing that no new legislation was needed to implement the key escrow encryption program.

- Should the Justice Department be required by law to report to Congress on those wiretaps in which key-escrow encryption was encountered and for which key components were released to a government agency?
- Should the Justice Department's new responsibilities for ensuring compliance with the key escrow procedures by State and local law enforcement authorities be codified in law?
- Should the Justice Department be required by law to give Congress a complete accounting of the number, use and location of the decrypt devices?
- Should procedures for changing an escrow agent be codified in law?

Answer 14. The Department of Justice does not see a need for legislation to deal with any of these matters. For example, the Department already expects that Congress will be made aware of wiretaps in which key-escrow encryption was encountered and for which key components were released. The Department expects to provide such information to the Administrative Office of the United States Courts for inclusion in the Office's annual report to the Congress on electronic surveillance under Title III and State statutes. With respect to electronic surveillance under FISA, the Department will provide such information as part of its FISA report to the intelligence oversight committees.

The Department does not anticipate difficulty with assuring State and local compliance with key component release procedures, particularly when the decryption capability rests exclusively in the hands of the Federal Government. With regard to the possible accounting for decrypt processors and their use and location, the Department does not object to providing such information to the Congress on a periodic basis. Finally, with regard to the selection of escrow agents, the Department believes that legislation to govern the process by which the Executive Branch might select an alternative escrow agent could hamper its ability to improve the system. Any selection of alternative escrow agents would, like the selection of the current agents, be preceded by appropriate consultation with the Congress.

Question 15. How will State and local law enforcement agencies access the key escrow system? Will every local Sheriff or police department that wants a decrypt device or the Chip Family Key get one?

Answer 15. The procedures for releasing key components for use in conjunction with wiretaps under State statutes are much the same as those for release of key components in conjunction with wiretaps under Title III or FISA. An important difference, however, is that requests for key components from State and local authorities cannot be submitted by law enforcement agencies; rather, they are to be submitted by the principal prosecuting attorney of the particular State or political subdivision. This not only significantly reduces the total number of entities that might make requests, but ensures that requests are made by high-level, usually elected officials, of the various jurisdictions.

As noted in the answer to an earlier question, the Administration recognizes that access to decrypt processors must remain carefully controlled. Among other things, key components will be released for use within a particular decrypt processor and will only be able to be decrypted and combined within that unit. Accordingly, careful control of the decrypt processors will contribute significantly to assurances of the integrity of the system.

Law enforcement agencies will not have access to the family key other than as programmed into the decrypt processor.

Question 16. Every Clipper Chip has the same Family Key programmed into it. When a wiretap intercepts conversations encrypted with Clipper Chip, law enforcement uses this Family Key to decode the intercepted serial number, or unique identifier, which the targeted chip sends out at the beginning of every conversation. With the serial number, the law enforcement agency can get the government's duplicate set of decoding keys from the escrow agents.

- Who has access to the Clip Family Key? Are they going to be distributed to all law enforcement agencies so they can quickly decipher serial numbers of chips that may become the target of a wiretap order?
- Will the Chip Family Key to all Clipper Chips be protected in any way and, if so, how?
- The Chip Family Key is built into the Chip when it is programmed and cannot be changed. In the event that someone got unauthorized access to the Chip Family Key, what could that person do with it?

Answer 16. With respect to the first question, access to the family key is very closely held. The family key is the combination of two binary numbers that are independently and randomly generated and held, respectively, by the Department of Justice and the FBI. The combined family key is held under tightly controlled conditions in a dual-control safe at the programming facility for use in the programming process. When needed for a programming run, the family key is extracted from storage by specially designated employees of the programming facility, in the presence of representatives of the escrow agents, and entered into the programmer. At the end of a programming run, the programmer is again cleared of the family key. In addition, the family key is programmed into decryption equipment so that such equipment can discern the particular chip ID number when necessary.

With respect to the question regarding availability of the family key to law enforcement agencies, the foregoing explanation indicates the extraordinary limitations on access to the family key. Law enforcement agencies desirous of learning whether a particular communication is encrypted with key-escrow encryption and, if so, learning the particular chip ID number will have access to the family key only as programmed into the decrypt processor. This may require a particular law enforcement agency not possessing such a processor to provide to an agency that does hold one the communications suspected of being encrypted, so that the initial determination can be made. It should be emphasized, however, that a law enforcement agency's determination of whether communications are being encrypted, and of the ID number of the chip performing the encryption, would occur in conjunction with the conduct of a lawfully authorized wiretap—not, as the question may imply, as part of activities preceding such authorization.

Notwithstanding the protections afforded the family key, access to that key is of only minimal value to a law enforcement agency. Apart from its ability to provide the law enforcement agency the ID number of a particular encryption chip, the family key, whether or not in the decrypt processor, is of no discernible value. The family key provides no access to the user's encrypted communications, nor does it make it any more possible for the law enforcement agency to conduct electronic surveillance of either encrypted or unencrypted communications.

Question 17. The Justice Department has assumed responsibility to "take steps to monitor compliance with the procedures." What steps will the Justice Department take to monitor compliance by state and local law enforcement authorities, who conduct the majority of wiretaps, to ensure that (a) the decrypt devices are adequately safeguarded and are deactivated when the authorization period ends; (b) the Chip Family Key is adequately safeguarded and (c) communications to the escrow agents are authentic?

Answer 17. The question correctly notes that the majority of criminal wiretaps are conducted by State and local law enforcement. If key-escrow encryption becomes widely used, one can infer that a significant proportion of the key component releases will be associated with wiretaps conducted under State statutes. It is, of course, of fundamental importance that escrowed keys are no more susceptible to improper use by State or local authorities than by Federal agencies.

(a) As noted earlier, the Department of Justice expects that, for some time, decrypt processors will be few in number and centrally maintained and controlled. In that event, it will be relatively easy to be assured that a decrypt processor is not diverted to an unauthorized person and that the decryption capability is terminated at the end of the authorized period of electronic surveillance. At a later time, should a State or local law enforcement agency be able to acquire and hold its own decrypt processor, we expect that the decrypt processor version will be one that will, among other things, (a) produce an electronic receipt for the key components transmitted to it, (b) have the capability of decrypting and combining only key components destined for that specific decrypt processor, and (c) automatically terminate its ability to decrypt the particular encryption chip. These technical characteristics, coupled with the continuing requirement that the key component request must come from the principal prosecuting attorney of a State or political subdivision, will offer great assurance against diversion of decrypt processors and unauthorized retention of decryption capabilities.

(b) With respect to the family key, the short answer is that the family key will not be available to State or local authorities, save within decrypt processors. Apart from its ability to provide the law enforcement agency the ID number of a particular encryption chip, the family key, whether or not in the decrypt processor, is of no discernible value to that agency. The family key provides no access to the user's encrypted communications.

(c) Requests from State or local authorities for release of key components are to come, not from law enforcement agencies, but from the principal prosecuting attorneys of the States or political subdivisions involved. The authenticity of such submissions can be confirmed by contact with the principal prosecuting attorney involved, which is expected to be a rather easy matter.

Question 18. American firms are allowed to export Clipper Chip devices to non-U.S. customers. What procedures are contemplated or in place to deal with requests by foreign law enforcement authorities for access to the keys to any Clipper Chip device being used abroad?

Answer 18. The Administration is according this issue careful consideration at this time. The Department of Justice believes that a number of important considerations would apply to any decision on whether to comply with a foreign country's request for assistance in decryption of key-escrow encrypted communications. For example, it will be important to know whether American citizens are targets of the electronic surveillance, and it will likely be important to know the reason for the electronic surveillance and the circumstances under which it was authorized, as well as whether the United States also has an interest in the electronic surveillance. It should also be noted that we may be able to assist the foreign country without providing it either decryption equipment or the key components for the particular encryption chip—by, for instance, decrypting the communications in this country and merely providing the decrypted text to the requester.

ANSWERS TO QUESTIONS FROM SENATOR PRESSLER TO ASSISTANT ATTORNEY GENERAL JO ANN HARRIS

Question 1. Why do you believe that private" manufacturers and users will purchase equipment which contains the Skipjack algorithm if that means the government can decode any encrypted messages, once it obtains the proper court approval?

Answer 1. Your question rightly notes that key-escrow encryption chips use the Skipjack algorithm, an algorithm substantially stronger than others now in common use; it is, for example, 16 million times stronger than the Data Encryption Standard (DES). The strength of the Skipjack algorithm makes key-escrow encryption chips attractive for use by the Federal Government in protecting sensitive unclassified information.

Likewise, we believe that it will make such chips attractive to the private sector, and for much the same reason; namely, that it is a remarkably strong protection against intrusion by eavesdroppers or even persons or entities engaged in corporate espionage. Most of us recognize that we will never be the targets of wiretaps and we do not fear that prospect. We do, however, worry about illicit interception of our communications, and strong encryption is excellent insurance against such activities.

In addition, we believe that many businesses will come to recognize the value of strong encryption that protects their proprietary information from unauthorized access, but does not permit their employees to engage with impunity in criminal ac-

tivities inimical to the firms' interest and law enforcement would be rendered helpless to investigate.

Question 2. What types of incentives does the Administration plan to use to encourage the use of the Clipper Chip? What are the future steps of implementation which the Administration proposes to take?

Answer 2. Various Executive Branch agencies are considering whether, and for what purposes, they may adopt key-escrow encryption and make it possible for persons outside the government to use key-escrow encryption for conducting secure communications with them. The Administration is also consulting with telecommunications equipment manufacturers regarding possible incorporation of key-escrow encryption in their products. In addition, the easy exportability of products equipped with key-escrow encryption should prove to be very attractive both to U.S. manufacturers of such equipment and to their customers.

Question 3. I understand the Administration is considering replacing one of the two escrow agents with a more neutral third-party, such as an entity in the Judicial branch or in the private sector. Which entities are being considered? What criteria must any prospective escrow agent have?

Answer 3. The Administration continues to look for ways to improve the key-escrow system. The system may be perceived to improve by the designation of at least one alternative escrow agent. Accordingly, the Administration is considering whether such an alternative should be designated and, if so, what must be done to effect such a designation. For example, an entity that is not part of a Cabinet Department may require legislative authority to serve as an escrow agent.

In selecting escrow agents, we looked for a number of important qualifications. Among other things, the candidates needed to:

- Be experienced in handling sensitive materials;
- Be familiar with communications and computer issues;
- Be able to respond quickly, and around the clock, when government agencies need to have encryption keys issued to them; and
- Be generally regarded by the public as both reliable and effective.

ANSWER TO A QUESTION FROM SENATOR MURRAY TO ASSISTANT ATTORNEY GENERAL JO ANN HARRIS

Question 1. In my office in the Hart building this February, I downloaded from the Internet an Austrian program that uses DES encryption. This was on a laptop computer, using a modem over a phone line. The Software Publishers' Association says there are at least 120 DES or comparable programs worldwide. However, U.S. export control laws prohibit American exporters from selling comparable DES programs abroad.

With at least 20 million people hooked up to the Internet, how do U.S. export controls actually prevent criminals, terrorists or whoever from obtaining DES encrypted software?

Answer 1. On the matter of export controls on encrypted software, the Department of Justice defers to the National Security Agency, which, we understand, has been asked the same question.

APPENDIX

KEY COMPONENT RELEASE PROCEDURES

Authorization procedures for release of encryption key components in conjunction with intercepts pursuant to title iii

The following are the procedures for the release of escrowed key components in conjunction with lawfully authorized interception of communications encrypted with a key-escrow encryption method. These procedures cover all electronic surveillance conducted pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Title III), Title 18, United States Code, Section 2510 *et seq.*

(1) In each case there shall be a legal authorization for the interception of wire and/or electronic communications.

(2) All electronic surveillance court orders under Title III shall contain provisions authorizing after-the-fact minimization, pursuant to 18 U.S.C. 2518(5), permitting the interception and retention of coded communications, including encrypted communications.

(3) In the event that federal law enforcement agents discover during the course of any lawfully authorized interception that communications encrypted with a key-escrow encryption method are being utilized, they may obtain a certification from the investigative agency conducting the investigation, or the Attorney General of the United States or designee thereof. Such certification shall:

(a) identify the law enforcement agency or other authority conducting the interception and the person providing the certification;

(b) certify that necessary legal authorization has been obtained to conduct electronic surveillance regarding these communications;

(c) specify the termination date of the period for which interception has been authorized;

(d) identify by docket number or other suitable method of specification the source of the authorization;

(e) certify that communications covered by that authorization are being encrypted with a key-escrow encryption method;

(f) specify the identifier (ID) number of the key-escrow encryption chip providing such encryption; and

(g) specify the serial (ID) number of the key-escrow decryption device that will be used by the law enforcement agency or other authority for decryption of the intercepted communications.

(4) The agency conducting the interception shall submit this certification to each of the designated key component escrow agents. If the certification has been provided by an investigative agency, as soon thereafter as practicable, an attorney associated with the United States Attorney's Office supervising the investigation shall provide each of the key component escrow agents with written confirmation of the certification.

(5) Upon receiving the certification from the requesting investigative agency, each key component escrow agent shall release the necessary key component to the requesting agency. The key components shall be provided in a manner that assures they cannot be used other than in conjunction with the lawfully authorized electronic surveillance for which they were requested.

(6) Each of the key component escrow agents shall retain a copy of the certification of the requesting agency, as well as the subsequent confirmation of the United States Attorney's Office. In addition, the requesting agency shall retain a copy of the certification and provide copies to the following for retention in accordance with normal recordkeeping requirements:

(a) the United States Attorney's Office supervising the investigation, and

(b) the Department of Justice, Office of Enforcement Operations.

(7) Upon, or prior to, completion of the electronic surveillance phase of the investigation, the ability of the requesting agency to decrypt intercepted communications shall terminate, and the requesting agency may not retain the key components.

(8) The Department of Justice shall, in each such case,

(a) ascertain the existence of authorizations for electronic surveillance in cases for which escrowed key components have been released;

(b) ascertain that key components for a particular key-escrow encryption chip are being used only by an investigative agency authorized to conduct electronic surveillance of communications encrypted with that chip; and

(c) ascertain that, no later than the completion of the electronic surveillance phase of the investigation, the ability of the requesting agency to decrypt intercepted communications is terminated.

(9) reporting to the Administrative Office of the United States Courts pursuant to 18 U.S.C. Section 2519(2), the Assistant Attorney General for the Criminal Division shall, with respect to any order for authorized electronic surveillance for which escrowed encryption components were released and used for decryption, specifically note that fact.

These procedures do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and noncompliance with these procedures shall not provide the basis for any motion to suppress

or other objection to the introduction of electronic surveillance evidence lawfully acquired.

Authorization procedures for release of encryption key components in conjunction with intercepts pursuant to state statutes

Key component escrow agents may only release escrowed key components to law enforcement or prosecutorial authorities for use in conjunction with lawfully authorized interception of communications encrypted with a key-escrow encryption method. These procedures apply to the release of key components to State and local law enforcement or prosecutorial authorities for use in conjunction with interceptions conducted pursuant to relevant State statutes authorizing electronic surveillance, and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, Title 18, United States Code, Section 2510 *et seq.*

(1) The State or local law enforcement or prosecutorial authority must be conducting an interception of wire and/or electronic communications pursuant to lawful authorization.

(2) Requests for release of escrowed key components must be submitted to the key component escrow agents by the principal prosecuting attorney of the State, or of a political subdivision thereof, responsible for the lawfully authorized electronic surveillance.

(3) The principal prosecuting attorney of such State or political subdivision of such State shall submit with the request for escrowed key components a certification that shall:

(a) identify the law enforcement agency or other authority conducting the interception and the prosecuting attorney responsible therefor;

(b) certify that necessary legal authorization for interception has been obtained to conduct electronic surveillance regarding these communications;

(c) specify the termination date of the period for which interception has been authorized;

(d) identify by docket number or other suitable method of specification the source of the authorization;

(e) certify that communications covered by that authorization are being encrypted with a key-escrow encryption method;

(f) specify the identifier (ID) number of the key-escrow chip providing such encryption; and

(g) specify the serial (ID) number of the key-escrow decryption device that will be used by the law enforcement agency or other authority for decryption of the intercepted communications.

(4) Such certification must be submitted by the principal prosecuting attorney of that State or political subdivision to each of the designated key component escrow agents.

(5) Upon receiving the certification from the principal prosecuting attorney of the State or political subdivision, each key component escrow agent shall release the necessary key component to the intercepting State or local law enforcement agency or other authority. The key components shall be provided in a manner that assures they cannot be used other than in conjunction with the lawfully authorized electronic surveillance for which they were requested.

(6) Each of the key component escrow agents shall retain a copy of the certification of the principal prosecuting attorney of the State or political subdivision. In addition, such prosecuting attorney shall provide a copy of the certification to the Department of Justice, for retention in accordance with normal recordkeeping requirements.

(7) Upon, or prior to, completion of the electronic surveillance phase of the investigation, the ability of the intercepting law enforcement agency or other authority to decrypt intercepted communications shall terminate, and the intercepting law enforcement agency or other authority may not retain the key components.

(8) The Department of Justice may, in each such case, make inquiry to:

(a) ascertain the existence of authorizations for electronic surveillance in cases for which escrowed key components have been released;

(b) ascertain that key components for a particular key- escrow encryption chip are being used only by an investigative agency authorized

to conduct electronic surveillance of communications encrypted with that chip; and

(c) ascertain that, no later than the completion of the electronic surveillance phase of the investigation, the ability of the requesting agency to decrypt intercepted communications is terminated.

(9) In reporting to the Administrative Office of the United States Courts pursuant to 18 U.S.C. Section 2519(2), the principal prosecuting attorney of a State or of a political subdivision of a State may, with respect to any order for authorized electronic surveillance for which escrowed encryption components were released and used for decryption, desire to note that fact.

These procedures do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and noncompliance with these procedures shall not provide the basis for any motion to suppress or other objection to the introduction of electronic surveillance evidence lawfully acquired.

Authorization procedures for release of encryption key components in conjunction with intercepts pursuant to FISA

The following are the procedures for the release of escrowed key components in conjunction with lawfully authorized interception of communications encrypted with a key-escrow encryption method. These procedures cover all electronic surveillance conducted pursuant to the Foreign Intelligence Surveillance Act (FISA), Pub. L. 95–511, which appears at Title 50, U.S. Code, Section 1801 *et seq.*

(1) In each case there shall be a legal authorization for the interception of wire and/or electronic communications.

(2) In the event that federal authorities discover during the course of any lawfully authorized interception that communications encrypted with a key-escrow encryption method are being utilized, they may obtain a certification from an agency authorized to participate in the conduct of the interception, or from the Attorney General of the United States or designee thereof. Such certification shall

(a) identify the agency participating in the conduct of the interception and the person providing the certification;

(b) certify that necessary legal authorization has been obtained to conduct electronic surveillance regarding these communications;

(c) specify the termination date of the period for which interception has been authorized;

(d) identify by docket number or other suitable method of specification the source of the authorization;

(e) certify that communications covered by that authorization are being encrypted with a key-escrow encryption method;

(f) specify the identifier (ID) number of the key-escrow encryption chip providing such encryption; and

(g) specify the serial (ID) number of the key-escrow decryption device that will be used by the agency participating in the conduct of the interception for decryption of the intercepted communications.

(4) This certification shall be submitted to each of the designated key component escrow agents. If the certification has been provided by an agency authorized to participate in the conduct of the interception, a copy shall be provided to the Department of Justice, Office of Intelligence Policy and Review. As soon as possible, an attorney associated with that office shall provide each of the key component escrow agents with written confirmation of the certification.

(5) Upon receiving the certification, each key component escrow agent shall release the necessary key component to the agency participating in the conduct of the interception. The key components shall be provided in a manner that assures they cannot be used other than in conjunction with the lawfully authorized electronic surveillance for which they were requested.

(6) Each of the key component escrow agents shall retain a copy of the certification, as well as the subsequent written confirmation of the Department of Justice, Office of Intelligence Policy and Review.

(7) Upon, or prior to, completion of the electronic surveillance phase of the investigation, the ability of the agency participating in the conduct of

the interception to decrypt intercepted communications shall terminate, and such agency may not retain the key components.

(8) The Department of Justice shall, in each such case,

(a) ascertain the existence of authorizations for electronic surveillance in cases for which escrowed key components have been released;

(b) ascertain that key components for a particular key-escrow encryption chip are being used only by an agency authorized to participate in the conduct of the interception of communications encrypted with that chip; and

(c) ascertain that, no later than the completion of the electronic surveillance phase of the investigation, the ability of the agency participating in the conduct of the interception to decrypt intercepted communications is terminated.

(9) Reports to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, pursuant to Section 108 of FISA, shall, with respect to any order for authorized electronic surveillance for which escrowed encryption components were released and used for decryption, specifically note that fact.

These procedures do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and noncompliance with these procedures shall not provide the basis for any motion to suppress or other objection to the introduction of electronic surveillance evidence lawfully acquired.

ANSWERS TO QUESTIONS FROM THE SENATE SUBCOMMITTEE ON TECHNOLOGY AND LAW TO NIST

Question 1. How long has the key escrow encryption standard been in development? Which agency originated these concepts?

Answer 1. The concept of key escrow has been in development, as a solution to meeting the needs for information protection while not harming the government's ability to conduct lawful electronic surveillance, for about five years. The final development and approval process of the Escrowed Encryption Standard (Federal Information Processing Standard 185) began following the President's decision announced on April 16, 1993. The concepts were developed at the National Security Agency, in response to requirements of law enforcement agencies and following discussions with NIST.

Question 2. Before NIST recommended the key escrow encryption method for nonclassified information, did it consider commercially-available encryption methods? If so, why were they rejected?

Answer 2. The voluntary key escrow encryption chip was developed specifically because no other products, commercial or otherwise, met the needs of the government for protecting its sensitive information in voice grade telephone communications while at the same time protecting its lawful electronic surveillance capabilities.

Question 3. The Administration recently established an interagency Working Group on Encryption and Telecommunications "to develop new encryption technologies" and "to review and refine Administration policies regarding encryption." Is this Group reviewing the Clipper Chip program?

Answer 3. This group is monitoring on-going development of the voluntary key escrow encryption initiative (e.g., alternative methods, better implementations, etc.). It is not reviewing the President's decision to commit the government to promote voluntary key escrow encryption for voice grade telephone communications.

Question 3.1. Has this Working Group yet recommended any changes to the Clipper Chip program? If so, what are those recommendations?

Answer 3.1. The Working group continues to pursue voluntary key escrow encryption technologies—and stands ready to work with interested industry firms to do so. It has not recommended any specific changes to the current program.

Question 3.2. What refinements to the Clipper Chip program is this Group considering?

Answer 3.2. It is examining organizations outside the CabinetDepartments to serve as alternative escrow agents. It is also examining issues involving international law enforcement cooperation on voluntary key escrow encryption matters.

Question 3.3. When will this Working Group complete its review of the Clipper Chip program?

Answer 3.3. While there is no re-examination of the Administration's commitment to the key escrow encryption initiative, the review of its implementation will likely

continue for some time. This reflects the need to monitor both the voluntary key escrow encryption program and other encryption developments.

Question 4. NIST is supposed to be leading efforts to work with industry to improve on the key escrow chips, to develop a key-escrow software and to examine alternatives to Clipper Chip. Could you describe NIST's progress on each of these three tasks? Specifically, what are the improvements and alternatives to Clipper Chip that NIST is considering?

Answer 4. The key escrow encryption software working group, which includes several industry representatives, has met several times to:

1) Specify and structure the problems to be solved;
2) Study the overall system integrity requirements for an acceptable solution;
3) Develop and list criteria for evaluating alternative proposed solutions; and
4) Begin defining software-based alternatives to the voluntary Clipper Chip key escrow system.

This research work can reasonably be expected to last at least two–three years.

Regarding hardware improvements, no working group has yet been formed, but the Administration has repeatedly expressed its willingness to work with interested industry participants to develop improvements and alternatives.

Question 5. The Defense Authorization Bill for Fiscal year 1994 has authorized $800,000 to be spent by the National Research Council of the National Academy of Sciences to conduct a two-year study of federal encryption policy. Do you think this study is necessary?

Answer 5. While we believe that the Administration's review of these issues was thorough, this study may identify new approaches for privacy while preserving lawful electronic surveillance capabilities which would be useful. The NRC's report will receive careful study.

Question 5.1. Why is the Administration not waiting to implement its key escrow encryption program until the National Research Council's study is completed?

Answer 5.1. The Administration's key escrow encryption initiative was announced on April 16, 1993, over seven months before the enactment of the National Defense Authorization Act for FY–94, which authorized the NRC study. The NRC study, which will consider issues substantially broader than those involved in key escrow encryption, will not be completed for at least two more years. The Administration's voluntary key escrow encryption initiative seeks to ensure that in setting new federal standards, lawful electronic surveillance capabilities are not undermined. Delaying our standards would harm federal agencies' capabilities to protect their information. Setting good encryption standards without key escrowing would harm lawful surveillance capabilities.

Question 5.2. Should this study be expedited?

Answer 5.2. NIST is not participating directly in the study, which is not yet underway. We do not know whether the study could be expedited without diminishing its thoroughness and accuracy.

Question 6. The Government wants the key escrow encryption standard to become the de facto industry standard in the United States, but has assured industry that use of the key escrow chips is voluntary. Would the Government abandon the Clipper Chip program if it is shown to be unsuccessful beyond Government use?

Answer 6. The key escrow encryption initiative successfully provides for excellent protection of federal information (and that of other users), without undermining the ability of law enforcement to conduct lawful electronic surveillance. Since it meets these goals successfully, the Escrowed Encryption Standard will continue to be a highly satisfactory method of protecting sensitive federal information and, therefore, should remain in effect regardless of its level of adoption within the private sector.

Question 7. If a user first encrypts a message with software using DES, and then transmits the message "double encrypted" with a key escrow chip, can you tell from looking at the cipher, or encrypted text, that the underlying message was encrypted?

Answer 7. No. The only way to tell that a message has been "double encrypted" in this way would be to decrypt the "outer layer" of encryption (i.e., that done with Clipper). Only then would one be able to tell that the message had first been encrypted with something else.

Question 8. Capstone is the Skipjack implementation for use with data transmitted electronically. Has the Capstone chip been incorporated in any product currently being marketed? When will the Capstone chip be released?

Answer 8. Capstone chips are just now becoming available. The Capstone chip is being incorporated into a personal computer memory card ("PCMCIA card") for use in providing security for sensitive government information in the Defense Message System. This is the only product actually in production using Capstone. The Cap-

stone chip technically can be used for many security applications, not just computer data.

Question 9. As computer and telecommunications technology advances, we are able to send more information at higher speeds. The speed and reliability of our telecommunications infrastructure gives American businesses the necessary edge in our global marketplace. The specifications for Clipper Chip indicate that it is designed to work on phone systems that transmit information no faster than 14,400 bits per second or on basic-rate ISDN lines, which transmit information at about 64,000 bits per second. Do the Clipper and Capstone Chips work fast enough for advanced telecommunications systems? Will Clipper Chip be able to keep up with the increasing speeds of telecommunications networks? Can the Skipjack algorithm be "scaled" to work at higher speeds?"

(See combined answer to questions 9 and 10 below.)

Question 10. Other commercially available encryption methods, like the Data Encryption Standard, have encryption rates much higher than Clipper Chip. Current high speed DES processors have encryption rates of approximately 200 million bits per second, which dwarfs the Clipper Chip's maximum throughput of 15 million bits per second. How will the Clipper Chip technology be able to compete with other encryption methods that can keep up with the higher speeds of emerging technologies?

Combined answer to Questions 9 and 10. The Clipper Chip as a hardware device was specially designed for end-to-end encryption of low-speed applications such as digitized voice. It is more than fast enough for this purpose, even if encrypted traffic is carried on the most advanced, high-speed telecommunications backbones. Capstone also was designed for end-to-end encryption of user data. Neither Clipper nor Capstone was designed to perform bulk encryption of high-speed telecommunications backbones.

The Skipjack algorithm, like the DES algorithm, is suitable for use at much higher speeds than implemented in Clipper and Capstone, and Skipjack-based hardware can be designed for higher-speed link-encryption applications as the need arises. As the speeds of the newest telecommunications technologies continue to grow, new key escrow devices will be developed as needed. Key escrow encryption technology will be able to compete with most other encryption methods for very high-speed applications.

Question 11. The Administration has assured industry that the key escrow technology will be enhanced to keep pace with future data requirements. What is the Administration doing to develop key escrow technology that can work with emerging high-speed communications technologies?

Answer 11. The Administration is working to identify needs for higher-speed applications of key escrow technology and will work to develop key escrow encryption devices to meet those needs. The technology for escrowing keys is readily adaptable to emerging high-speed applications.

Question 12. Openly available devices, such as Intel-compatible microprocessors, have seen dramatic gains, but only because everyone was free to try to build a better version. Given the restrictions on who can build key escrow encryption chips, how will these chips keep up with advances in semiconductor speed, power, capacity and integration?

Answer 12. Despite the requirements that a firm must meet to produce key escrow encryption chips, we expect that there will be a number of manufacturers competing against each other to produce the best product, and that such competition will drive them to keep up with the latest technological advances. It is worth noting that only a few companies can produce the sophisticated microprocessors you reference, yet the competition in that market has driven them to achieve remarkable advances in that technology.

Question 13. NIST estimates the cost of establishing the key escrow facilities to be $14 million and the cost of operating the key escrow facilities will be about $16 million annually. What is your statutory authority for these expenditures?

Answer 13. Under the Computer Security Act of 1987, NIST is responsible not only for developing Federal Information Processing Standards for the protection of sensitive federal government information, but also for providing assistance in using the Standards and applying the results of program activities under the Act.

Most directly applicable are sections 278g–3(b) (1) and (3) of title 15 of the U.S. Code. Subsection (3) authorizes NIST to provide technical assistance in implementing the Act to operators of federal systems. Subsection (1) authorizes NIST to assist the private sector in "using and applying" the results of NIST's programs under the Act, thus showing that the scope of the assistance authorized by the Act includes help in applying the standards NIST develops. This section indicates that NIST may

provide technical assistance to the private sector rather than just to the federal agencies that must comply with the standards.

Question 14. What has been spent to date on Skipjack, Capstone and Clipper Chip?

Answer 14. NIST's FY–94 expenditures through the end of April are approximately $268,000. FY–93 expenditures regarding the Clipper Chip and key escrow encryption technologies involved a significant portion of NIST's computer security budget, specifically the level of resources devoted to this technology was approximately four years of professional staff time and travel expenses of about $10,000. NSA will provide their funding information separately to the Committee.

No cost figure can be assigned to the NSA's development of the SKIPJACK algorithm, in part because it was developed as a family of classified algorithms over a period of years.

Question 15. NIST has explained that the single company manufacturing the Clipper Chips was selected because of its expertise in designing custom encryption chips, as well as its secure facilities and employees with high security clearances. How long will it take for the Government to certify another vendor of Clipper Chip? What progress, if any, has the Administration made on finding another vendor?

Answer 15. Several firms have expressed interest in becoming vendors of key escrow encryption chips. So far, one of these (other than the current company) has demonstrated that it has the technical expertise, secure facilities, and cleared personnel necessary to do the job. We expect that this firm would be able to commence production by early 1996.

Question 16. Once a given chip has been compromised due to use of the escrowed keys, is there any mechanism or program to re-key or replace compromised hardware? Is there any method for a potential acquiring party to verify whether the keys on a given chip have been compromised?

Answer 16. It should be emphasized that release of escrowed key components to law enforcement agencies for use in conjunction with lawfully authorized electronic surveillance does not constitute compromise of the particular chip associated with those key components. Upon completion of electronic surveillance, the law enforcement agency's ability to decrypt communications with the particular chip ends, and therefore, those communications again become undecryptable unless and until the key components are released once more. There is no way to re-key chips for which escrowed keys have been used. If a chip could be re-keyed, it might be possible for users to replace the chip unique key, thus defeating the law enforcement access field. The hardware can be replaced with new hardware for which keys have not been released from escrow.

Question 17. The Skipjack algorithm itself is classified, but the halves of the keys held by the escrow agents cannot be since they will be released upon presentation of a court order. Will the databases maintained by the escrow agents to hold the keys be subject to the Freedom of Information Act? What exception will you rely upon to justify withholding requests for information under FOIA?

Answer 17. As a matter of clarification, it should be noted that the key components are not themselves part of the SKIPJACK algorithm, nor do they, in combination with each other or with any other group of binary numbers, generate the algorithm, or provide any information regarding its characteristics.

We understand your question regarding the Freedom of Information Act as relating to the electronically stored key components held by NIST as an escrow agent, which information associates each particular chip-unique ID number with one of the components of its unique key. Release of these key components would permit a FOIA requestor to circumvent the protections that NIST is required to develop and promulgate as Federal Information Processing Standards under the Computer Security Act of 1987 (P.L. 100–235). Under 5 U.S.C. 552(b)(2), agencies are authorized to withhold information the disclosure of which would risk the circumvention of a statute or agency regulation. Therefore, the key escrow materials are protectible under 5 U.S.C. 552(b)(2).

Question 18. Normal security procedures involve changing cryptography keys periodically, in case one has been compromised. For example, those of us who use E-mail systems are accustomed to periodically changing our password for access to the system. But Clipper Chip's family and unique key cannot be changed by the user. If these keys are compromised, it will not matter how frequently the user changed their session keys. Does the long use of the same family and unique keys increase the likelihood that these keys will be compromised while they are still in use? Does this eliminate a significant degree of the user's control of the level of security that the system provides?

Answer 18. No. As discussed in the answers to other questions, access to the key escrow components will be highly controlled. In addition, these components them-

selves will be encrypted. Extensive audit procedures have been designed into the system to guard against any unauthorized access. Given these and other extensive protections, it is very unlikely that long use of the same chip unique or family key will have any negative impact upon users' security.

Question 19. How secure is the Clipper Chip if someone gets unauthorized access to half the key?

Answer 19. Knowledge of only one key component provides no information about the chip unique key and, therefore, does not in any way harm the security of the user.

Question 20. Every Clipper Chip has the same Family Key programmed into it. When conversations encrypted with Clipper Chip are intercepted, this Family Key is used to decode the intercepted serial number, or unique identifier, which the targeted chip transmits at the beginning of every conversation. With the serial number, the law enforcement agency can get the government set of key components from the escrow agents. Who has access to the Chip Family Key? Is it going to be distributed to all law enforcement agencies so they can quickly decipher serial numbers of chips that may become the target of a wiretap order? Will the Chip Family Key be protected in any way and, if so, how?

Answer 20. With respect to the first question, access to the family key is very closely held. The family key is the combination of two binary numbers independently and randomly generated and held, respectively, by the Department of Justice and the FBI. The combined family key is held under tightly controlled conditions in a dual-control safe at the programming facility for use in the programming process. When needed for a programming run, the family key is extracted from storage by specially designated employees of the programming facility, in the presence of representatives of the escrow agents, and entered into the programmer. At the end of a programming run, the programmer is again cleared of the family key. In addition, the family key is programmed into all law enforcement decrypt processors to discern the particular chip ID number when necessary.

With respect to the question regarding availability of the family key, the foregoing explanation indicates the extraordinary limitations on access to the family key. Agencies desirous of learning whether a particular communication is encrypted with key escrow encryption and, if so, learning the particular chip ID number will have access to the family key only as programmed into the decrypt processor. This may require a particular agency not possessing such a processor to provide to an agency that does hold one the communications suspected of being encrypted, so that the initial determination can be made. It should be emphasized, however, that an agency's determination of whether communications are being encrypted, and of the ID number of the chip performing the encryption, would occur in conjunction with the conduct of a lawfully authorized surveillance—not, as the question may imply, as part of activities preceding such authorization. Further questions on the protection of the family key are best directed to the U.S. Department of Justice.

Question 21. The Chip Family Key is built into the chip when it is programmed and cannot be changed. In the event that someone got unauthorized access to the Chip Family Key, what could that person do with it?

Answer 21. In the very unlikely event that someone were able to gain access to the family key and were able to figure out a means to use it, the only information that could be obtained would be the serial numbers of the EES devices used for a telecommunication. Of course, intercepting such a telecommunication without lawful authorization would be a felony offense.

Question 22. Clipper Chip design data will need to be released to manufacturers in order for them to incorporate the chip into security devices. How will we be assured that this design information, in itself, will not allow the key escrow chips to be compromised?

Answer 22. The only design data which will need to be released to manufacturers of devices using the chip are its interface specifications, such as size, power requirements, data input, and the like. None of these data can in any way be used to determine the encryption algorithm or any other information affecting the security of the encryption.

Question 23. A decrypt device will be used to receive an electronic transmittal of the two key halves from the escrow agents. The decrypt device will then be able to decrypt the intercepted message, until the wiretap authorization ends, when it will automatically turn itself off. How many of these decrypt devices will be built? Will the decrypt devices be maintained in a central secure facility? If so, who will maintain custody of the devices and how will they be distributed to the law enforcement agencies that need them?

Answer 23. Termination of a decrypt processor's ability to decrypt communications using a particular key escrow chip is a fundamental protection built into the system

and law enforcement agencies that have received key components will be required to certify such termination. In the prototype model of the decrypt processor, that termination is effected manually; automatic termination will be available in later versions.

The number of decrypt processors that will ultimately be produced will probably be in large measure a function of the number of key escrow equipped devices in use throughout the country and the number of times key escrow encryption is encountered in the course of wiretaps. For the foreseeable future, when it is likely that the number of decryption processors will be small, it is likely that they would be centrally held by the FBI, to be made available for use in the field on an as-needed basis.

Question 24. The key escrow approach is designed to ensure the ability of the American government to access confidential data. What would make key escrow chips manufactured in America an attractive encryption method for foreign customers?

Answer 24. The key escrow initiative was undertaken to provide users with robust security without undermining lawfully authorized wiretaps. This point is important to emphasize as the market for this product very much depends on who users perceive as a threat to intercept their communications.The potential export market for encryption products can be divided into two categories: exports for foreign government use and exports for non-government use. The most likely government users of commercial encryption products would be countries that have a relatively low degree of technical sophistication, lack other resources necessary to develop their own encryption products, and do not perceive the United States as a primary threat. Such countries might be primarily concerned about access to their communications by neighboring countries, terrorists, criminal elements, or domestic political opponents. Such government users might view a vulnerability to possible eavesdropping by the United States as a price worth paying in return for security against those more immediate threats. However, we do not expect such users to constitute a major export market for key escrow encryption products.

The non-government sector represents a much greater potential export market for key escrow encryption products. While some prospective users abroad may steer clear of key escrow products because the United States will retain access, there may be many who believe they are unlikely to be targeted by U.S. intelligence in any case or for whom the superior security offered by key escrow encryption products against threats of greater concern may make key escrow products an attractive option. (For example, a distributor of pay-TV programming may depend on encryption to ensure that only those viewers who pay for the service can decrypt the TV signal. Such a distributor probably would not be concerned about the threat of access by the United States Government, and might favor key escrow encryption over competing products that use weaker encryption algorithms.) In addition, others may be attracted to key escrow encryption products in part by the need to interoperate with other users of such products, especially businesses in the United States.

Question 25. If key escrow chips are not commercially accepted abroad, and export controls continue to restrict the export of other strong encryption schemes, is the U.S. Government limiting American companies to a U.S. market?

Answer 25. U.S. firms have long been major players in the international commercial encryption market despite export controls on encryption products. We do not impose a blanket embargo on products which encrypt data or voice. Encryption products undergo a one-time technical review, the results of which are used in decisions as to whether a given product can be exported to particular end users consistent with U.S. interests. After the one-time review, products are given expedited licensing treatment. Some are licensed for export to virtually all end users. Some products are licensed less widely. Overall, over 95% of export license applications for encryption products are approved. Any encryption product can be exported by U.S. businesses for use in their facilities abroad. In addition, the President recently directed that a number of changes be made in the licensing process to expedite licensing and to ease the regulatory burden on exporters. In short, we have every reason to expect that the U.S. will continue to be a major exporter of commercial encryption products, regardless of the commercial success of key escrow encryption products.

Question 26. Is the key escrow encryption system compatible with existing encryption methods in use?

Answer 26. As is true among devices using different algorithms (e.g., DES, RSA, RC4, etc.) key escrow encryption products will not interoperate with other products using a different algorithm. Note also that many commercial products that use the same algorithm do not interoperate due to other constraints (e.g., transmission rates, voice-digitization process, other protocols, etc.).

Question 27. As part of NIST's continuing review of the key escrow encryption scheme, is NIST considering any new encryption approach that would be compatible with the embedded base of equipment?

Answer 27. No new approaches are being considered with the specific goal of compatibility with some installed devices. Note that no encryption approach would be consistent with the entire installed base of equipment. It is too widely varied.

*Question 28.*Critics of U.S. export restrictions on strong encryption technology argue that these restrictions have the effect of reducing the domestic availability of user-friendly encryption, which could otherwise be routinely incorporated in software and telecommunications equipment. What is the Administration's response to this criticism?

Answer 28. We do not believe that export controls have reduced the domestic availability of encryption. Encryption products have been commercially available in this country for a long time, especially since the adoption of the Data Encryption Standard (DES) as a Federal Information Processing Standard in 1977. However, demand for such products has been limited, with government purchases comprising the bulk of the encryption market. As public interest in and understanding of the need for security increases, we are moving aggressively to make available to the public, on a voluntary basis, the voluntary key escrow encryption technology needed to provide strong encryption without sacrificing the public's interest in effective law enforcement. Far from reducing the domestic availability of encryption, government actions, from adopting the DES standard to development of key escrow encryption technology, and even in driving the market during the years when there was little commercial interest, have greatly increased the domestic availability of encryption products, rather than reducing it.

Answer to a Question From Senator Patty Murray to NIST

Question 1. In my office in the Hart building this February, I downloaded from the Internet an Austrian program that uses DES encryption. This was on a laptop computer, using a modem over a phone line. The Software Publishers' Association says there are at least 120 DES or comparable programs worldwide. However, U.S. export control laws prohibit American exporters from selling comparable DES programs abroad. With at least 20 million people hooked up to the Internet, how do U.S. export controls actually prevent criminals, terrorists or whoever from obtaining DES encryption software?

Answer 1. On the matter of export controls on encryption software (including DES), NIST defers to the National Security Agency, which, we understand, has been asked the same question.

Answer to a Question From Senator Larry Pressler to Raymond Kammer, Deputy Director, NIST

Question 1. NIST has approved the use of the Clipper Chip as the federal standard for encoding federal communications involving sensitive but unclassified information. Is there a reason why the Clipper Chip is not approved for classified information as well? If so, please explain.

Answer 1. The National Security Agency approves encryption systems for the protection of classified information, and is considering approval of Clipper for selected classified applications. The encryption algorithm used in the Clipper Chip, called SKIPJACK, is one of a family of encryption algorithms developed by NSA for use in protecting classified information.

Answers to Questions From the Senate Subcommittee on Technology and the Law to Whitfield Diffie

Question 1. The serial number, or unique identifier number, for each key escrow chip is sent out as a header on each encrypted communication. If the Government just wanted to know where I was and not what I was saying, would it be possible for the Government to track down the header on my communications and figure out where I was from where I was sending out my encrypted messages? Could you explain how this would be possible? Do you have concerns about this?

Answer 1. The serial number is contained in a block encrypted with the Family Key and is thus accessible only to those who can obtain the Family Key. This point is discussed further in the response to question 8.

Concealing the gross characteristics of messages (existence, timing, length, origin, destination, etc.) is typically more difficult to achieve by *end-to-end* techniques

(those that operate only in the user's equipment) than concealing their contents. In modern telephone systems the called and calling numbers of phone calls are typically easy to get at. (This is what makes possible the controversial Caller-ID service.) In electronic mail—even encrypted electronic mail—this information is normally contained in the message headers. In the case of cellular telephones, the particular characterists of the phone as a radio (*Emitter ID*) can be detected and used to distinguish among individual phones.

In short, although preventing interceptors from detecting serial numbers would be one necessary step in preventing tracking, that task is quite difficult and serial numbers may not be the most critical element.

Question 2. NIST has stated that "industry interest in developing secure software based on key escrow encryption is minimal." Is that a correct assessment and, if so, could you explain why?

Answer 2. NIST's statement is unfamiliar to me, but certainly accords with my experience. We do not perceive our customers as wanting escrowed encryption, so why would we want to develop software around it? There are *de facto* industry standards growing up around public key and multiple-DES. I suspect I speak for a broad segment of the industry in saying that we prefer to develop software based on publicly known techniques that are receiving acceptance from our customers.

Question 3. In a speech last month at a telecommunications conference in Buenos Aires, Vice President Gore described his vision for a global information network to link the people of the world and provide a global information marketplace. How would the electronic information flow between countries be effected if other countries will not let Clipper Chip in?

Answer 3. At present most internet traffic, like most of the world's communications, is unencrypted. It is the belief of those of us who support improvement of telecommunication security that the developing information infrastructure will not be able to serve its function adequately unless it is made more secure. Since the network—like the world economy—is international, worldwide interoperability standards are required. Security products that are the exclusive property of one country, or even a small group, of countries, would appear to have no possibility of fulfilling this function.

Question 4. We are market leaders in applications software and operating systems. Our world leadership in operating systems is dependent on integrating security in internationally distributed systems. If overseas companies provide systems based on algorithms without key escrow schemes that encrypt faster and more securely, how will we compete internationally?

Answer 4. If overseas companies produce operating systems and application programs based on security mechanisms that cannot be exported from the United States, the U.S. software business will surely suffer.

Question 5. The National Security Agency has stated that "many non-key escrow encryption products have long been licensed for export * * * [and] * * * will continue to be * * *." Do you share this view that many American encryption products are freely licensed for export?

Answer 5. You have quoted NSA as saying that products "have been licensed for export" and "will continue to be." They have said nothing about "freely." In our experience it is often difficult and time consuming to get export licenses in secure communications and related areas even when there are comparable foreign products or when licenses have previously been granted for similar shipments.

The history of export licenses, however, is a question of facts not of views and these are facts to which I have little access. The question points up an issue that should be high on the export reform agenda: An opening up of the export control process that creates a written public record of export control policies and decisions.

Question 6. The Administration has stated that the Skipjack algorithm in the Clipper Chip must remain classified and only specially certified vendors will be given access to it. By contrast, openly available devices, such as Intel-compatible microprocessors, have seen dramatic gains, but only because everyone was free to try to build a better version. Given the restrictions on who can build Clipper devices, do you have any concerns about how Clipper will keep up with advances in semiconductor speed, power, capacity and integration?

Answer 6. I do, but these concerns are merely part of a larger concern. If the semi-conductor industry becomes dependent on parts available only on the sufferance of the government, it will no longer be free to make and carry out basic business decisions.

Should NSA (which appears to have control of the technology and the supply of parts despite the fact that key escrow is a Department of Commerce standard) decide to cease authorizing the production of clipper chips, industry would no longer be able to ship products interoperable with those sold earlier.

When Digital Equipment Corporation concluded some years ago that a very high speed DES device might be needed, it developed one internally using Gallium Arsenide technology. Should a semi-conductor manufacturer decide that a similar high-speed SKIPJACK chip was required it would need NSA's concurrence and cooperation to go ahead with the product. Under these circumstances, it might be blocked because NSA did not have any way of tamper proofing a sufficiently fast design. It should also be noted that such developments could be blocked or delayed even when they were completely in accord with government policy and objectives, because of lack of government funds, personnel, or other resources.

Question 7. The Administration has assured industry that the key escrow technology will be enhanced to keep pace with future data requirements. Are you aware of anything the Administration is doing to develop key escrow technology that can work with emerging high-speed communications technologies?

Answer 7. It is my understanding that a high speed algorithm called BATON is under development, but I have no further information.

Question 8. Every Clipper Chip has the same Family Key programmed into it. This Family Key is used by law enforcement to decode an intercepted serial number, or unique identifier, that is transmitted at the beginning of every encrypted conversation. The law enforcement agency presents this serial number to get the decoding keys from the escrow agents. In the event that someone got unauthorized access to the Chip Family Key, what could that person do with it? Do you have any concerns about who will have access to the Chip Family Key?

Answer 8. Although the administration seems to be saying that the Family Key will be very tightly controlled, it is traditional COMSEC doctrine that nothing that remains constant for a long period of time can be expected to remain secret. This is the view under which cryptographic systems are always presumed to be known to an opponent.

Possession of the family key, together with the LEAF creation method, would allow an opponent to identify individual cryptographic chips as discussed under question 1. It would also bring an opponent one step closer to recovering Chip Unique Keys, as described in my testimony, and thus having potential access to all past and future messages encrypted by particular chips.

Question 9. The Internet Privacy Enhanced Mail (PEM) is becoming an internationally recognized system for encrypting Electronic Mail over the Internet. If the Administration is successful in making the Skipjack key escrow system an American standard for encrypting electronic mail while the rest of the world uses PEM, how would this effect encrypted E-mail traffic between the U.S. and other countries?

Answer 9. I don't know how widely PEM is used at present, either inside or outside the U.S. PEM, in contrast to its competitor Pretty Good Privacy or PGP, has a rigid certificate structure that requires the construction of certification hierarchies and registration of users. The effect is to require top down adoption of PEM rather than promoting its free spread among users. This has slowed its "market penetration." PEM is also export controlled, although I have been told there are non-U.S. implementations.

At present only the DES/RSA combination of cryptosystems are reflected in PEM standards. PEM is potentially flexible, however, attaching labels to messages that indicate the cryptosystem in use. (Sun's implementation, for example, allows alternate cryptosystems.) There has been discussion of expanding PEM to allow triple DES and a key escrow based version seems equally possible.

Nonetheless, if a multiple DES and RSA version of PEM is widely used outside the U.S. and a key escrow version is used within, this will present a major barrier to secure communications between American and foreign companies.

Question 10. Is the demand for strong encryption technology growing and, if so, why?

Answer 10. It is hard to distinguish a demand for *strong* encryption from a demand for encryption period. It is, after all, rare for someone to want *weak* encryption. Usually it is accepted because strong encryption is too expensive or otherwise unavailable. The long history of scrambled (weakly analog encrypted) telephones, for example, was a result of the high cost of digitizing the sound so that it could be strongly encrypted.

That said, the demand for encryption is growing. The fundamental reason is that as the quality of communication networks improves, the value of the traffic they carry increases. At one time long distance telephone calls were too expensive and too poor in quality to be used for anything more than making appointments or getting quick answers to questions. Today, entire business meetings are conducted by phone. The growth in quality and cost performance of written electronic communications has been even greater and has lead to important and sensitive message being

transmitted by fax or electronic mail. Today, most of these messages go without "envelopes." That is what encryption provides.

SUN MICROSYSTEMS COMPUTER CORP.,
Mountain View, CA, May 23, 1994.

Hon. PATTY MURRAY,
Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR SENATOR MURRAY: I very much appreciate the opportunity to respond to your question:

Question 1. In my office in the Hart building this February, I downloaded from the Internet an Austrian program that uses DES encryption. This was on a laptop computer, using a modem over a phone line. The Software Publishers' Association says there are at least 120 DES or comparable programs worldwide. However, U.S. export control laws prohibit American exporters from selling comparable DES programs abroad.

With at least 20 million people hooked up to the Internet, how do U.S. export controls actually prevent criminals, terrorists or whoever from obtaining DES encrypted software?

Answer 1. I have considered this issue with some care and I believe the answer lies in the critical dependence of the adoption of security measures on their ease of use.

No matter how obvious the need for communication security is to those of us who work in the field, it is difficult to sell. The reason for this is that communications intelligence is rarely visible to its target. Even if a company finds that it is repeatedly loosing bids by small margins to a single competitor, discovering whether the vulnerability is in communications or procedures or personnel is very difficult. Under the circumstances, selling secure communications is much like selling insurance against a disaster that the customer cannot see.

The result is that users tend to avail themselves of secure communications only when security is built in as an automatic function that does not interfere with their work or require their attention. The availability of a cryptographic program that is not integrated into an application is useful only to those already dedicated to the practice of security. For these people, converting the Federal Standard for DES or some similar algorithm specification into a program is a small part of the job.

Consider for example, someone who is writing many drafts of a report and keeping them encrypted by using a file encryption program separate from the word processor. The writer must not only remember to reencrypt the file after each editing session, but if the word processor leaves unintended copies around on the disk, must run a disk cleaning program as well. Any slip-up potentially leaves the document vulnerable to compromise and similar examples present themselves in communication.

What NSA fears is a Sun or Microsoft or DEC operating system with encryption built in in such a way that after an initial log-in, all security is provided transparently for the user. This might, for example, support an application allowing people at remote locations to work jointly on a document. All drafts would be communicated encrypted without the writers having to do anything.

The answer to your question is thus twofold. The U.S. export controls probably do not prevent criminals or terrorists who are attentive to security from getting access to encryption software. They may, for a time, prevent these people from getting what honest business people want: Encryption software that functions automatically and invisibly in their operating systems and supports a variety of application programs in a consistent way.

From a communications intelligence viewpoint, NSA's fear is rational. Because the software marketplace is international, however, the effect of export controls has been to stifle the development of security in operating systems. Companies whose markets are frequently more than half foreign are loathe to expend resources developing features that can be sold to only a minority of their customers.

Concern with America's position in international trade is also rational, however. It seems unlikely that businesses can indefinitely increase their dependence on computers and communications without installing security mechanisms commensurate with the value of their investments. The security machinery itself will be a small fraction of the total revenue for computer systems and software, but its smooth inte-

gration into operating systems and applications may be the *sine qua non* of future market acceptance.

Yours truly,

WHITFIELD DIFFIE,
Distinguished Engineer.

SUN MICROSYSTEMS COMPUTER CORP.,
Mountain View, CA, May 23, 1994.

Hon. PATRICK J. LEAHY,
Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR SENATOR LEAHY: I very much appreciate both the opportunity of speaking before your subcommittee and the opportunity to respond to your questions, the answers to which I have attached to this letter.

As I sat listening to the committee proceedings, I felt a glimmer of hope that the key escrow proposal might actually be stopped. At the same time I realized that winning this "fight," should we be so lucky, would not contribute to winning the larger battle: The battle to improve the security of American business and personal communications.

For more than a decade, we have been trying without much success to persuade the public that their communications are worth protecting and that this protection is worth paying for. In this campaign, we have usually had little support from NSA and at times we have had active opposition. NSA, however, has a decisive role to play and the battle probably cannot be won without it.

NSA is in possession of a vast body of information about both the vulnerabilities of communications and actual instances of their exploitation. When it is in marketing mode, as it was during the mid-nineteen eighties with its STU–III and CCEP programs, it lends its weight to be view that the communication's of Americans are being exploited and need protection. When it is arguing against commercial standards or the relaxation of export controls, it takes the opposite view.

In undertaking the key escrow program, NSA has put forth a deal. They will lend both their technical and marketing abilities to the development of a new generation of widely available security equipment. The condition is the key escrow. Most of NSA's budget goes to intelligence and intelligence demands its cut. Should the key escrow program be stopped, it seems likely that we will return to a situation in which industry must try to persuade the public of the need for security over NSA's opposition or at best in the face of its indifference.

I suggest, therefore, that should Congress choose to take over the reigns of policy in this area, it will not be sufficient to end the Administration's venture into key escrow. It will be necessary to insist that protecting the communications of all Americans be put foremost among NSA's responsibilities and to mandate NSA's full and unreserved participation in this program.

Yours truly,

WHITFIELD DIFFIE,
Distinguished Engineer.

ANSWERS TO QUESTIONS FROM THE SENATE SUBCOMMITTEE ON TECHNOLOGY AND THE LAW TO STEPHEN T. WALKER

Question 1. The serial number, or unique identifier number, for each key escrow chip is sent out as a header on each encrypted communication. If the government just wanted to know where I was and not what I was saying, would it be possible for the government to track down the header on my communications and figure out where I was from where I was sending out my encrypted messages? Could you explain how this would be possible? Do you have concerns about this?

Answer 1. It would be relatively straightforward for the government to track the movement of individuals and the phone numbers of people with whom they are communicating using the Clipper key escrow system without the need for a wiretap court order.

The law enforcement decryption unit that is used to initially detect the use of a Clipper device contains the "family key" of all Clipper telephone security devices. This key allows the decryption unit to identify the unique serial number without any interaction with the key escrow centers. Anyone with access to such a decryption unit could identify calls from specific Clipper devices without a court order.

Such activity would require access to phone communications facilities that would normally be associated with court-ordered wiretaps. Access to the decryption unit would normally be reserved for law enforcement officials [Initially there is only one such unit, but presumably if Clipper becomes widely used, there will be many available to law enforcement throughout the country.]

It is important to note that if one does not use a TSD, one's communications are trivially vulnerable to this same threat today.

Question 2. You are a member of the Computer System Security and Advisory Board, which was created by the Computer Security Act of 1987 to advise NIST on computer policy matters. Was this Board consulted by NIST during consideration of the key escrow encryption standard?

Answer 2. The Board was never consulted "before-the-fact" in any of the Administration's announcements on Clipper, the Digital Signature Standard, the Escrow Encryption Standard or any other matter related to cryptography. In each case the members of the Board were as surprised as the general public by these announcements.

As was demonstrated in the case of the proposed licensing of the Digital Signature Algorithm to Public Key Partners last June, the advice of the Board relative to the cost impact on the general public eventually lead to a reversal of that proposal. Had the advice of the Board been sought before this proposal was put forward, I believe at least nine months of delay in issuing the Digital Signature Standard could have been saved. Given that the government has delayed the issuing of the DSS for over twelve years, though, it is not clear that this would have made much difference.

It is important to note that all activities of the Board except those dealing with budgets and proprietary concerns must be held in open session. Under these circumstances, describing its proposed actions to the Board would be equivalent to the government announcing its actions in public. I do believe that if the government wanted to it could make use of the proprietary information provisions to seek the advise of the Board prior to announcing its policy decisions. It is apparent that the government has chosen not to take this course in every announcement related to cryptography.

Question 3. Many users prefer encryption *software* because it is more cost effective than a hardware solution. So far, Clipper Chip has not been implemented in software. NIST announced in February that it will try to establish cooperative partnerships with the software industry to develop key escrow software. You are a member of NIST's Software Escrowed Working Group, which is examining the possibilities for alternatives to Clipper Chip. Has any progress been made? If not, could you explain why?

Answer 3. I am a member of the NIST Software Escrow Encryption Working Group and just this past week, I have made a proposal to NIST and NSA of an alternative to Clipper key escrow that I believe provides as good a solution to the law enforcement concerns while being implementable entirely in software. This proposal could provide a far more cost-effective solution to key escrow than Clipper. I made this proposal in the interests of demonstrating that key escrow could be achieved without secret encryption algorithms and mandatory hardware.

I must reiterate the major concern of my testimony before your hearing that government-imposed key escrow in any form, whether implemented in Clipper hardware or in software, should not take place until it has been subjected to full legislative review, passage of a law, signed by the President, and if necessary, determined to be Constitutional by the Supreme Court.

My suggestion that at least one software key escrow approach is just as good as that envisioned in Clipper is made as a technical suggestion for consideration by the government in full recognition that the government may choose to impose this technique on the American people without the benefit of Congressional consideration. I sincerely hope this does not happen.

Question 4. NIST has stated that "industry interest in developing secure software based on key escrow encryption is minimal." Is that a correct assessment and, if so, could you explain why?

Answer 4. The statement in quotes in this question is a complex statement that must be treated in parts. I believe that industry is concerned about key escrow for many reasons. Key escrow implemented in hardware using Clipper represents a significant increase in the complexity and cost of their products. Even key escrow implemented in software will complicate products while not adding to their marketability.

More importantly, I am convinced that industry has little interest in developing key escrow encryption techniques, whether in hardware or software, for exactly the same reason as most Americans citizens: they don't like it. If we as a people decide that the benefits of key escrow are worth the risks to individual privacy, if we pass

legislation making key escrow legal under controlled circumstances, then I believe most Americans and most of American industry will support its implementation in computer and telephone products. Until then, I believe the opposition to key escrow will continue.

Question 5. In a speech last month at a telecommunications conference in Buenos Aires, Vice President Gore described his vision for a global information network to link the people of the world and provide a global information marketplace. How would the electronic information flow between countries be affected if other countries will not let Clipper Chip in?

Answer 5. I have thought a great deal about the international aspects of key escrow, whether by Clipper or in software. I do not see any practical way in which key escrow is ever going to work in a multinational setting. I believe that individual governments may work out ways for sharing the results of law enforcement intercepts in foreign countries. But I see no way that multinational companies will be able to communicate with their customers and suppliers in foreign countries if each government imposes its own form of key escrow. Vice President Gore's vision of a global information marketplace will be impossible so long as the U.S. Government or any other government feels key escrow is essential to their law enforcement interests. If the U.S. persists in this, it may have a national information marketplace, but it will be locked out of the international marketplace.

Question 6. We are market leaders in applications software and operating systems. Our world leadership in operating systems is dependant on integrating security in internationally distributed systems. If overseas companies provide systems based on algorithms without key escrow schemes that encrypt faster and more securely, how will we compete internationally?

Answer 6. We are rapidly reaching the point where we cannot compete internationally in products that incorporate good quality security. Multinational companies are requiring such capabilities in the information systems they are buying, and we are being locked out of those sales. And these are not just sales of encryption products. They involve all aspects of word processing, spreadsheets, integrated office products, database management systems, the very heart of our information system industry. We are not able to compete in these security-conscious marketplaces, and increasingly this will affect both our market share and our own abilities to protect U.S. sensitive information.

Question 7. In your testimony you note that the Skipjack algorithm works fast enough to encrypt phone and low speed computer communications but will not "easily scale to meet the needs of high speed computer communications." Could you explain this limitation in the underlying algorithm for Clipper Chip?

Answer 7. This question has a complex answer that involves the way key escrow will be used as well as its implementation in hardware.

First, the problem I was referring to is not a limitation of the Skipjack algorithm but relates to the hardware technologies currently being used to implement Clipper and Capstone. Some people have stated that the current versions will have to be reimplemented to work at the higher speeds required by modern computer communications.

But the nature of key escrow of individual communications requires interaction on a per-phone call or per-computer message basis. This is best done at the user end of the communications links (the individual phones or computers originating the communications). The present implementations of Clipper and Capstone are well-suited to this use.

There are other uses of cryptography that require much higher bandwidth and are not amenable to individual key escrow. Bulk encryption of high bandwidth communications links requires very fast cryptography. The Skipjack algorithm could probably be implemented with much higher speed technology for such uses. But key escrow of individual phone calls or computer messages is not meaningful in high bandwidth bulk encryption applications.

If the American people agree that we need key escrow, Skipjack, with its embedded key escrow, will play a role in achieving that capability. But key escrow is not the answer to all our cryptographic needs. We will also need cryptographic technologies that will operate at the same speeds as our highest bandwidth communications. For these devices, key escrow makes no sense.

Question 8. The National Security Agency has stated that "many non-key escrow encryption products have long been licensed for export * * * [and] * * * will continue to be: Do you share this view that many American encryption products are freely licensed for export?

Answer 8. There are many encryption products made in the U.S. with "weak" cryptography that are approved for export from the U.S. The best example is the so called "SPA deal" of 1992 in which the government agreed to the export of prod-

ucts containing cryptography so long as the key length used was 40 bits or less (the key length of the Data Encryption Standard is 56 bits).

Unfortunately, key lengths of 40 bits or less are, with today's technology, trivially easy to defeat. When U.S. companies attempt to sell products based on 40-bit keys to their foreign customers who already have 56-bit DES products, they generally fail.

As the use of good quality cryptography continues to grow, those U.S.. products that have weak cryptography (and are therefore approved for export) will lose any market share that may now exist.

Question 9. The administration has stated that the Skipjack algorithm in the Clipper Chip must remain classified and only specially certified vendors will be given access to it. By contrast, openly available devices, such as Intel-compatible microprocessors, have seen dramatic gains, but only because everyone was free to try to build a better version. Given the restrictions on who can build Clipper devices, do you have any concerns about how Clipper will keep up with advances in semiconductor speed, power, capacity and integration?

Answer 9. This is a fundamental question at the core of technological advances throughout our society. If the last twenty years have shown anything, it is that open development of technologies that compete directly in the marketplace will be far more successful than closed designs. This is true for personal computers and for cryptographic devices.

Classified encryption algorithms that must be designed and implemented in closed communities will never be able to compete with the open-market development of products based on DES and similar public algorithms. Key escrow does not require the use of classified algorithms; it will work equally well with DES or other popular algorithms. If the Administration insists on a closed development and implementation process, it will relegate its key escrow ideas to a very small segment of the overall market for cryptography.

Question 10. The Administration has assured industry that the key escrow technology will be enhanced to keep pace with future data requirements. Are you aware of anything the Administration is doing to develop key escrow technology that can work with emerging high-speed communications technologies?

Answer 10. No, but I believe there are many techniques that can be used to attempt to make key escrow work with high speed communications. See my answers to questions 7 and 9.

Question 11. Every Clipper Chip has the same Family Key programmed into it. This Family Key is used by law enforcement to decode an intercepted serial number, or unique identifier, that is transmitted at the beginning of every encrypted conversation. The law enforcement agency presents this serial number to get the decoding keys from the escrow agents. In the event that someone got unauthorized access to the Chip Family Key, what could that person do with it? Do you have any concerns about who will have access to the Chip Family Key?

Answer 11. If an unauthorized individual obtained access to a device family key, that individual could create a capability to track the users of any device in that family, as was discussed in question 1. I believe that the procedures being established for protection of family keys and device escrow keys are quite strong. But as was pointed out by Senator Specter, it is not easy to keep a secret over a long period of time.

Question 12. The Internet Privacy Enhanced Mail (PEM) is becoming an internationally recognized system for encrypting Electronic Mail over the Internet. If the Administration is successful in making the key escrow chips an American standard for encrypting electronic mail while the rest of the world uses PEM, how would this affect encrypted E-mail traffic between the U.S. and other countries?

Answer 12. If key escrow were to become a mandatory standard in the U.S. while the rest of the world continued to use Internet PEM, there would be very little encrypted e-mail between the U.S. and the rest of the world.

Question 13. Is the demand for strong encryption technology growing and, if so, why?

Answer 13. Concern for the protection of sensitive information from unauthorized disclosure, modification or destruction is growing in all segments of the information technology market, from individuals to large corporations and governments. The demand for good quality cryptography will continue to grow until this concern can be adequately addressed. This is a fundamental issue that the Administration's policies of always siding with the law enforcement and national security interests continue to ignore. People will find ways to protect their sensitive information even if they have to buy encryption products from foreign sources.

Answers to Questions From the Senate Subcommittee on Technology and The Law to Vice Admiral J.M. McConnell

Question 1. The Defense Authorization Bill for Fiscal Year 1994 has authorized $800,000 to be spent by the National Research Council of the National Academy of Sciences to conduct a study of federal encryption policy. Can we wait to implement the key escrow encryption program until we have the benefit of the NRC's study? Do you think this study is necessary? Should this study be expedited?

Answer 1. We do not believe that we can wait until after the NRC study is completed in 1996 to begin implementation of the key escrow initiative. The information technology industry is dynamic and fast-moving, and to wait another two years or more would, we believe, jeopardize the success of the initiative. Industry demand for encryption products is growing, and the technology is available now to meet that demand with encryption products that provide an outstanding level of security to the user without making it impossible for law enforcement agencies to conduct lawful wiretaps. To wait for the completion of the NRC study would make it much more likely that the market would turn to other encryption products which would defeat lawful wiretaps. We believe that such a delay would not be in the best interest of the American people.

Neither do we believe that the study should be expedited. For our part, we will carefully consider the conclusions of the NRC study. We expect that it will give very careful consideration to the issues, and we would not want the pressure of an unnecessarily short deadline to limit the study group's ability to produce the best report possible.

Question 2. The Administration has said that it is continuing to restrict export of the most sophisticated encryption devices, in part, "because of the concerns of our allies who fear that strong encryption technology would inhibit their law enforcement capabilities." Do we really need to help our allies by prohibiting the export of strong American encryption products, since those same countries can simply control the encryption bought within their borders?

Answer 2. Exports of encryption products are subject to review primarily to protect U.S. national interests, including national security, law enforcement, foreign policy, and other important interests. The law enforcement concerns of our allies are a consideration, especially as the ability of our allies to combat terrorism, drug trafficking, and other international law enforcement problems can have direct benefits to the United States. However, foreign law enforcement concerns do not drive our export control policy. We would continue to review encryption exports to protect U.S. national interests even if foreign law enforcement concerns disappeared.

Question 3. Do you know whether foreign governments would be interested in importing key escrow encryption products to which they hold the decoding keys?

Answer 3. Several foreign governments have expressed interest in key escrow encryption technology due to their own law enforcement concerns. There have been some preliminary discussions, but issues such as who would hold the escrowed keys and the circumstances of government access to escrowed keys must be fully vetted.

Question 4. The Government wants the key escrow encryption standard to become the de facto industry standard in the United States. Would the Government abandon the Clipper Chip program if it is shown to be unsuccessful beyond government use?

Answer 4. We do not expect the program to be unsuccessful beyond government. We have developed a sound security product that we expect will find many uses in government information systems and further believe that government use will bring with it a commercial market, particularly in the defense sector. We have developed a sound security product that we expect will find many uses in government information systems regardless of its success in commercial markets.

Question 5. Openly available devices, such as Intel-compatible microprocessors, have seen dramatic gains, but only because everyone was free to try to build a better version. Given the restrictions on who can build devices with the classified Skipjack algorithm, how will key escrow chips keep up with advances in semiconductor speed, power, capacity and integration?

Answer 5. Despite the requirements that a firm must meet to produce key escrow encryption chips, we expect that there will be a number of manufacturers competing against each other to produce the best product, and that such competition will drive them to keep up with the latest technological advances. It is worth noting that only a few companies can produce the sophisticated microprocessors you reference, yet the competition in that market has driven them to achieve remarkable advances in that technology. NSA's STU–III secure telephone program provides an example of a cryptographic product line that keeps pace with technology.

The presence of a classified algorithm does not preclude keeping pace with technology. Through NSA's use of a competitive, multi-vendor approach, STU–III secure telephone products have continued to evolve in response to user requirements and technological advances despite their use of a classified encryption algorithm and the consequent need for security restrictions on the manufacturers.

Question 6. How well does the Skipjack algorithm work on telecommunications operating at very high speeds? Is NSA working on another algorithm, called BATON, that could be used at high speeds with a key escrow system? Will Capstone be compatible with BATON?

Answer 6. Using currently available microelectronics technology, the SKIPJACK algorithm could not be used for encryption at very high speeds. BATON is the name of an algorithm developed by NSA that could be used at higher rates of speed. We have no plans to develop key escrow encryption devices using BATON, however. Instead, we are considering another algorithm for use at high speeds with a key escrow system.

A high-speed key escrow device based on an algorithm other than SKIPJACK would not be "compatible with Capstone" in the sense that traffic encrypted by such a device could not be decrypted by Capstone, and vice versa. However, since such a device would be used for much higher-speed applications than those for which Capstone was designed, there would be no need for it to be compatible with Capstone in that sense.

Question 7. Can Capstone be used to encrypt video programming? If so, have cable companies been approached by any government agency to use Capstone to scramble or encrypt cable programs?

Answer 7. Capstone could be used to encrypt any digital signal, including video programming, operating at up to about 10 million bits per second. It could be used for encrypting individual video channels but not for bulk encryption of many channels multiplexed together in a single link. NSA is not aware of any government agency approaching cable companies to urge the use of Capstone. Two manufacturers have asked us about the suitability of key escrow devices for this purpose, however.

Question 8. Encryption software is available that can be used with Clipper to encrypt a message before or after it has been encrypted with Clipper. This "double encrypting" risks bypassing the key escrow feature. If a sender first encrypts the message with software using DES, and then transmits the message "double encrypted" with Clipper, can you tell from looking at the cipher, or encrypted text, that the underlying message was encrypted?

Answer 8. The only way to tell that a message has been "double encrypted" in this way would be to decrypt the "outer layer" of encryption, i.e. that done with Clipper. Only then would one be able to tell that the message had first been encrypted with something else.

ANSWERS TO QUESTIONS FROM SENATOR PRESSLER TO VICE ADMIRAL J.M. MCCONNELL

Question 1. Admiral as you are aware, critics of the Administration's proposal argue that as a practical matter, no criminal, foreign spy, or terrorist of any sophistication would be foolish enough to use an encryption device designed by the NSA and approved by the FBI. How do you respond? Why do[n't you] think the people whose telecommunications the NSA and the FBI want most to decode will be the very people most unlikely to use this technology?

Answer 1. From what we know today, the overriding requirement that spies, terrorists, and criminals have is for readily available and easy to use equipment that interoperates. Key escrow encryption is not meant to be a tool to catch criminals. It will make excellent encryption available to legitimate businesses and private citizens without allowing criminals to use the telecommunications system to plan and commit crimes with impunity. We believe it would be irresponsible for government to make excellent encryption broadly available knowing that its use by criminals would make it impossible for law enforcement agencies to conduct lawful wiretaps against them.

The Department of Justice credits information gleaned through wiretaps as leading to more than 20,000 felony convictions since the early 1980s. This would not have been possible if the criminals had been using encryption systems the FBI could not break.

Without government action, however, this fortunate situation will change. At present most people, and most criminals, don't use encryption. However, there is an increasing public awareness of the value of encryption for protecting private per-

sonal and business communications. Increasing demand for encryption by the public will likely lead to the widespread use of some form of standardized encryption on the public telecommunications network.

This development would have great benefits for the country. Legitimate businesses and private individuals could use the telecommunications system secure in the knowledge that their private information such as business records and credit card numbers could not be intercepted by third parties.

But there is a down side. Criminals, terrorists, and others could also use the system to plan crimes, launder money, and the like, completely secure in the knowledge that law enforcement agencies could not listen to those communications. Just as legitimate businesses operate much more efficiently and effectively using the telecommunications system than they could without it, so will criminal enterprises be able to operate more efficiently and effectively if they no longer have to avoid using the telecommunications system.

The United States is faced with a choice. We can sit back and watch as the emerging national information infrastructure becomes a valuable tool for criminals and terrorists to use to plan and carry out their activities with complete security, or we can take steps to maintain the current ability of government to conduct lawful wiretaps so that prudent criminals will have to find other less efficient ways to operate and foolish ones may be caught. Key escrow encryption is the latter option.

Question 2. Would widespread use of the Skipjack algorithm harm U.S. exports? Do you think it is unlikely foreign businesses will purchase American encryption technology if the U.S. Government holds a set of the decoding keys?

Answer 2. I do not believe that widespread use of key escrow encryption in the United States will harm U.S. exports. If it has any effect at all, it could increase exports somewhat. Key escrow encryption products provide another option for foreign purchasers that they have not had in the past; to the extent that foreigners do purchase key escrow encryption products, it will mean an increase in exports. Meanwhile, U.S. exporters are free to continue to sell the products they currently sell in foreign markets and to seek license approvals for new products.

It is difficult to predict the foreign market for U.S. key escrow encryption technology. Businesses that fear U.S. Government interception of their communications presumably would avoid products for which the U.S. Government holds keys. However, there are a number of reasons why foreign businesses might purchase them. One major reason would be to communicate securely with U.S. businesses that use them. In addition, the superior level of security provided by key escrow products (against all but lawful U.S. Government access) may make them attractive to foreign businesses that do not view U.S. Government access as a major concern. While some prospective users abroad may steer clear of key escrow products because the United States will retain access, there may be many who believe they are unlikely to be targeted by U.S. intelligence in any case or for whom the superior security offered by key escrow encryption products against threats of greater concern may make key escrow products an attractive option. For example, a distributor of pay-TV programming may depend on encryption to ensure that only those viewers who pay for the service can decrypt the TV signal. Such a distributor probably would not be concerned about the threat of access by the United States Government, and might favor suitable key escrow encryption products over competing products that use weaker encryption algorithms.

Question 3. You were present when the previous panelist, Stephen Walker, described how present U.S. laws prohibit his company from exporting encryption products. As I understand it, Senator Murray's bill, S. 1846, attempts to relax these export controls somewhat. Please give us your views on this legislation.

Answer 3. I support the Administration's position, as announced by the White House on February 4, that current export controls must remain in place and that regulatory changes should be implemented to speed exports and reduce the licensing burden on exporters. The bill you reference appears to be inconsistent with the Administration position. I would be happy to provide you further information on the Administration's reasons for maintaining the current export controls in an appropriate setting.

ANSWER TO A QUESTION FROM SENATOR MURRAY TO VICE ADMIRAL MCCONNELL

Question 1. In my office in the Hart building this February, I downloaded from the Internet an Austrian program that uses DES encryption. This was on a laptop computer, using a modem over a phone line. The Software Publishers' Association says there are at least 120 DES or comparable programs worldwide. However, U.S. export control laws prohibit American exporters from selling comparable DES pro-

grams abroad. With at least 20 million people hooked up to the Internet, how do U.S. export controls actually prevent criminals, terrorists, or whoever from obtaining DES encryption software?

Answer 1. Serious users of encryption do not entrust their security to software distributed via networks or bulletin boards. There is simply too much risk that viruses, Trojan Horses, programming errors, and other security flaws may exist in such software which could not be detected by the user. Serious users of encryption, those who depend on encryption to protect valuable data and cannot afford to take such chances, instead turn to other sources in which they can have greater confidence. Such serious users include not only entities which may threaten U.S. national security interests, but also businesses and other major consumers of encryption products. Encryption software distribution via Internet, bulletin board, or modem does not undermine the effectiveness of encryption export controls.

○

ISBN 0-16-047780-8